

e·quinux



**VPN Tracker 7
Manual**

© 2013 equinix AG and equinix USA, Inc. All rights reserved.

Under copyright law, this manual may not be copied, in whole or in part, without the written consent of equinix AG or equinix USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinix logo is a trademark of equinix AG and equinix USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

equinix shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of this document or any change to the router in general, including without limitation, any lost profits, business, or data, even if equinix has been advised of the possibility of such damages.

Photo credit: mem-film.de / photocase.de (page 25)

Every effort has been made to ensure that the information in this manual is accurate. equinix is not responsible for printing or clerical errors.

Revised June 28, 2013

Created using Apple Pages.

www.equinix.com

Contents

Introducing VPN Tracker.....	5	Network Scanner.....	30
What's New?	6	Accounting	33
VPN Tracker Editions.....	8	Exporting Connections.....	34
Getting Started	9	Troubleshooting.....	38
Installing VPN Tracker	9	Reference	43
Activating VPN Tracker	9	Settings Reference	43
Migrating from Previous Versions	11	Basic Tab	43
Getting Connected.....	12	Advanced Tab	50
VPN Crash Course	12	Actions Tab	57
The Big Picture	13	Export Tab	57
Setup for an Existing VPN	16	VPN Tracker Preferences	58
Setup without Configuration Guide	17	Secure Desktop Reference.....	61
Importing Connections	19	Accessing Files & Printers over VPN	67
Connecting to Your New VPN	20	L2TP / PPTP Connections	69
Working with VPN Tracker	21	VPN and Network Address Translation (NAT)	70
Secure Desktop: Your VPN Cockpit	22	Certificates and Smart Cards.....	73
VPN Productivity	26	Choosing the Right VPN Device	80
Managing Connections and Secure Desktops	26	Further Resources	81
VPN Connection Stats	27	Keyboard Shortcuts.....	82
Menu Bar Item	27		
Notifications	27		
Actions	28		
Notes	29		

VPN Tracker 7 at a Glance

Search PRO
If you're a consultant with lots of customers, you'll appreciate being able to filter your connection list to find *that* VPN.

Secure Desktop
Everything you need to work over VPN in one place: Applications, servers, websites and more.

On/Off Switch
Connect and disconnect your VPN by sliding its switch on or off.

Network Traffic
See what's happening on your VPN connection.

Add Items
Add a new VPN connection, group or Secure Desktop

Toggle Details
Display or hide your connection details or the traffic graph.

Network Scanner PRO
Explore the remote network and instantly connect to services.

Accounting PRO
Keep track of your connection time.

Log
Get troubleshooting advice and see what VPN Tracker is doing.

Configuration
Set up your VPN or change settings.

Status
Your VPN at a glance – see your assigned IP address, the remote network address, contact information and notes.

Contacts & Notes
Jot down notes and store the admin contact for the VPN or the billing reference number for a client.

Technical Support
No matter where you are, technical support is just one click away!

Introducing VPN Tracker

Welcome to VPN Tracker, the leading VPN client on Mac. Whether you are new to VPN or a seasoned VPN guru, this manual will help you get started with VPN Tracker.

New to VPN Tracker?

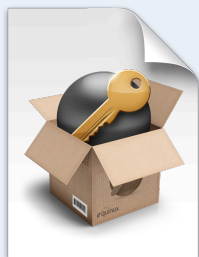
- ▶ Install VPN Tracker and get a free trial in → *Getting Started*
- ▶ Take our → *VPN Crash Course* and then → *Get Connected*
- ▶ Find out how using your VPN is a breeze with → *Secure Desktop*

Upgrading to VPN Tracker 7?

- ▶ See how to → *Upgrade Your License* and how VPN Tracker automatically takes care of → *Migrating from Previous Versions*
- ▶ Explore → *What's New in VPN Tracker 7*

System Administrators and IT Departments

- ▶ Connect to your existing VPN or set up a VPN from scratch in → *Getting Connected*
- ▶ Set up VPN Tracker for others in → *Exporting Connections*
- ▶ Use the → *Settings Reference* for in-depth configuration information



VPN Tracker Deployment Guide

- ▶ Are you deploying VPN Tracker to end users in your organization?
- ▶ Are you a consultant setting up VPN Tracker for your clients?
- ▶ Are you managing the VPN Tracker licenses in your organization?

Get the VPN Tracker Deployment Guide for up-to-date information and best practices. Download your free copy today at <http://www.vpntracker.com>

Conventions Used in This Document

Links to External Websites

Sometimes you will be able to find more information on external websites. Clicking links to websites will open the website in your web browser:

<http://equinux.com>

Links to Other Parts of this Manual

A → *Link* will take you to another place in the manual. Simply click it if you are reading this manual on your computer.

Tips and Tricks



This manual contains lots of great tips. You can easily spot them by looking for the light bulb icon.

Advice for Setting up Your VPN Gateway



If you are setting up not just VPN Tracker, but also a VPN gateway, this icon points out recommended settings and things you need to pay attention to when setting up a VPN gateway.

Warnings



This exclamation mark warns you when there is a setting or action where you need to take particular care.

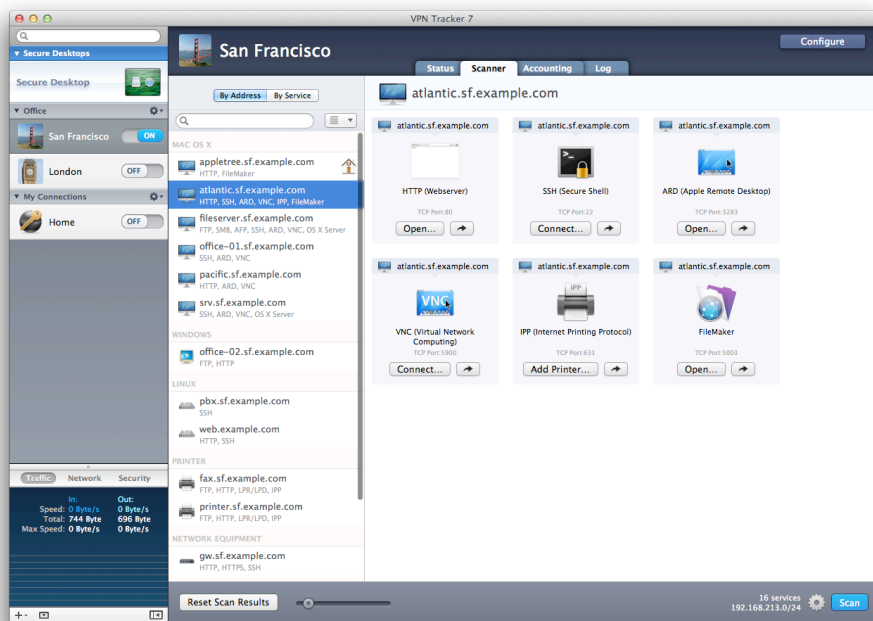
Getting Help

VPN Tracker makes VPN simple. However, computer networking and VPNs can be complex and tricky at times, so we have also built in tools and helpful features that will assist you if you ever run into problems. Check out → *Troubleshooting* for more information.

What's New?

Network Scanner **PRO**

Explore the remote network, instantly connect to services, and assist clients.



Streamlined UI with separate areas for setup and everyday tasks

Free up space in your Dock and **hide VPN Tracker's Dock icon**, customize your workspace with **detachable log windows**, and **re-open** with exactly the windows and VPNs that you left off at.

Got a brand new Mac this year? VPN Tracker's **Retina graphics** look gorgeous on your shiny new display!

PRO For consultants and pros with a large number of VPNs, the new **condensed layout** and built-in **search** make it easy to locate that particular VPN.

Security Boost

All algorithms are now available in all editions of VPN Tracker – use **AES-256**, **SHA-2**, **DH groups 14-18** and **smart cards**, even with your home setup (compatible VPN gateway required).

Even Easier to Use

Stuck setting up the VPN? There's now **built-in help for every single setting**. And if you got a setting wrong, the improved log can now not only tell you where the problem is, but which the **correct setting** would be.

If you're using a **one-time passcode** system such as RSA SecurID, new XAUTH settings let you customize how VPN Tracker requests your passcode.

Accounting **PRO**

Keep track of your connection time for easier billing and work tracking.

DNS Improvements

Remote DNS servers can now be configured for **reverse DNS lookup**, and the new **DNS lookup tool** lets you see exactly what is going on.

Updated Secure Desktop

Stuck connecting to a **file server**? Secure Desktop now makes it easy to use the correct settings. **Microsoft Remote Desktop** connections also work with **CoRD**. And for power users, many Secure Desktop items can now be customized even further.

Improved Export & Deployment

New export settings let you decide **whether user's are permitted to store their passwords**. And VPN Tracker now ships as an installer package, making it easy to **integrate with 3rd party deployment solutions**.

64-Bit from Start to Finish

All components of VPN Tracker are now 64-bit, so VPN Tracker can benefit from the performance and security improvements OS X provides for 64-bit applications.

Edition Changes

VPN Tracker Personal and Player Edition are now VPN Tracker

We've combined the features of VPN Tracker Personal and Player Edition to create a single streamlined VPN Tracker 7 that works with any VPN setup – including those using **strong encryption** and **multiple remote networks**.

An even more powerful VPN Tracker Pro

For power users, consultants and network administrators, VPN Tracker 7 Pro features the brand new **Network Scanner**, a new **Condensed Layout, Accounting, Search**, and of course **Export** and **Network-to-Network** connections.

Upgrading to VPN Tracker 7

If you currently own VPN Tracker, you can easily upgrade to VPN Tracker 7 and take advantage of all these great new features.

To see your upgrade options, choose VPN Tracker 7 > Buy VPN Tracker in the demo, or visit

<http://www.equinux.com/goto/upgradevpntracker>

The License Manger will show you all available VPN Tracker license upgrades.

VPN Tracker Editions

We offer two different editions of VPN Tracker to fit your requirements. Find out which edition is right for you.

VPN Tracker

VPN Tracker is designed for individual users and for end users in corporate environments. It's perfect for getting connected to an office or home network.

VPN Tracker Pro

VPN Tracker Pro adds advanced features for consultants, network admins and power users.



Regardless of the edition you have purchased, you can always download and use the same copy of the VPN Tracker application. Your license will automatically unlock all the features included in your edition.

Do I need VPN Tracker Pro?

VPN Tracker Pro is a great asset if you are a consultant, a system or network administrator, or are working with multiple VPN connections:

- ▶ Export VPN connections for yourself and other users.
- ▶ Scan the remote network for services or to assist users.
- ▶ Connect to multiple VPNs at the same time.
- ▶ Manage a large number of VPNs using search, a condensed layout, and connection groups.
- ▶ Configure your Mac as a router to provide the entire network with a VPN tunnel using Network to Network connections.
- ▶ Control your OS X L2TP/PPTP VPN right within VPN Tracker.

VPN Tracker Editions Compared

	VPN Tracker	VPN Tracker Pro
Connectivity		
Connect to one VPN	✓	✓
Connect to multiple VPNs at the same time	–	✓
Connect two sites (Network to Network)	–	✓
Integration of OS X PPTP/L2TP VPN	–	✓
Export		
Export	–	✓
Organization		
Organize your connections in groups	–	✓
Use a condensed layout	–	✓
Search for connections	–	✓
Accounting	–	✓
Tools		
Ping Tool	✓	✓
DNS Lookup Tool	✓	✓
Network Scanner	–	✓

Getting Started

This chapter shows you how to install VPN Tracker, and how to activate your license. If you do not have a license yet, don't worry – we'll also show you how to get a demo key to try VPN Tracker for free.

Installing VPN Tracker

You can always download the latest version of VPN Tracker from the VPN Tracker website:

<http://vpntracker.com/download>

There is one single download for all editions of VPN Tracker.

Once your download has finished, double click the downloaded "VPN Tracker 7.pkg" installer package, if it doesn't open automatically. Then simply follow the steps to install VPN Tracker 7.



Opening VPN Tracker

Go to your Applications folder in Finder and double-click VPN Tracker 7 to open it.

If you previously had VPN Tracker 6 or 5 installed on your Mac, VPN Tracker may prompt for an administrator password to make your existing connections available in VPN Tracker 7.

Activating VPN Tracker

Activating VPN Tracker is quick and easy. You can activate your license in a few seconds over any Internet connection.

How many licenses do I need?

VPN Tracker is licensed per-machine, so each Mac you want to run VPN Tracker on will need its own license. Licenses can be bought in the equinix Online Store or at your nearest equinix reseller. You can find your nearest reseller with our Reseller Locator:

<http://equinix.com/goto/reseller>

Testing VPN Tracker

If you want to make sure VPN Tracker works with your connection and meets your expectations before purchasing, you can request a free demo license. This will give you access to all VPN Tracker Pro features (except exporting connections). Simply click the button to obtain a demo license when you first open VPN Tracker.



If you set up your VPN connection during your free demo period, VPN Tracker will keep all your settings and details once you activate a purchased license.

Once you're satisfied VPN Tracker suits your needs, you can purchase a full license right from within VPN Tracker.

To purchase a license:

- ▶ Select VPN Tracker 7 > Buy VPN Tracker from the menu bar
- ▶ Follow the instructions to purchase a license. Your license will be activated immediately.

If you prefer, you can also purchase VPN Tracker in our Online Store:

<http://equinux.com/goto/buyvpntracker>

Activating a License from the equinux Online Store

To activate a license bought in our online store:

- ▶ Open VPN Tracker. In case you still have time left on your demo period, choose “VPN Tracker 7 > Activate VPN Tracker” from the menu bar on top of your screen.
- ▶ If you are asked for your equinux ID and password, enter the equinux ID and password that was used for the purchase.
- ▶ If you own more than one license, you will be asked to select the one that you would like to activate.
- ▶ Follow the steps to complete activation

Activating Using an Activation Code

If you received an activation code:

- ▶ Open VPN Tracker. In case you still have time left on your demo period, choose VPN Tracker 7 > Activate VPN Tracker from the menu bar on top of your screen.
- ▶ Enter the activation code.
- ▶ Follow the steps to complete activation.



You might be prompted to enter a name and email address. This will make it easier for you to keep track of who is using which license – particularly useful if you have a large number of VPN users in your organization.

Changing Computers

If you'd like to change computers, you can easily move your license:

- ▶ Choose VPN Tracker 7 > Deactivate VPN Tracker from the menu bar on your old Mac.
- ▶ Once deactivated, you'll be able to activate your new Mac straight away. Simply follow the activation instructions above.
- ▶ Enjoy your new Mac!

Broken Mac? Stolen Mac?

If your old Mac is broken or unavailable, enter your activation code (or equinux ID and password) on the new Mac, and select the option to reset your license, or use the license manager to revoke your activation code.

Managing Licenses

If you are in charge of VPN Tracker licenses at your company, our [License Manager](#) can help you deploy, move and manage those licenses.



VPN Tracker Deployment Guide

- ▶ Are you deploying VPN Tracker to end users in your organization?
- ▶ Are you a consultant setting up VPN Tracker for your clients?
- ▶ Are you managing the VPN Tracker licenses in your organization?

Get the VPN Tracker Deployment Guide for up-to date information and best practices. Download your free copy today at <http://www.vpntracker.com>

Migrating from Previous Versions

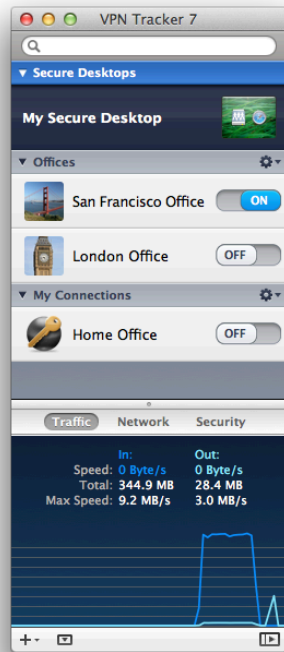
No matter which version you are coming from, it's easy to migrate all your settings to VPN Tracker 7 to continue working without interruption.



If you are evaluating VPN Tracker 7, don't worry – **your existing connections and settings in previous versions of VPN Tracker remain untouched.**

VPN Tracker 6 (and 5)

Your existing connections and settings are automatically migrated to VPN Tracker 7 when you open it for the first time.



If you ever want to migrate your connections again, you can tell VPN Tracker to repeat the migration to ensure you have the latest connections and settings from VPN Tracker 5 or 6: "File > Migrate from VPN Tracker 5/6". Please note that this migration will replace all connections in VPN Tracker 7

VPN Tracker 4 (and 3)

You can migrate connections from these versions of VPN Tracker from the File menu (File > Migrate...).

You will find your migrated connections in their own connection group named "VPN Tracker 4" (or "VPN Tracker 3") in VPN Tracker.

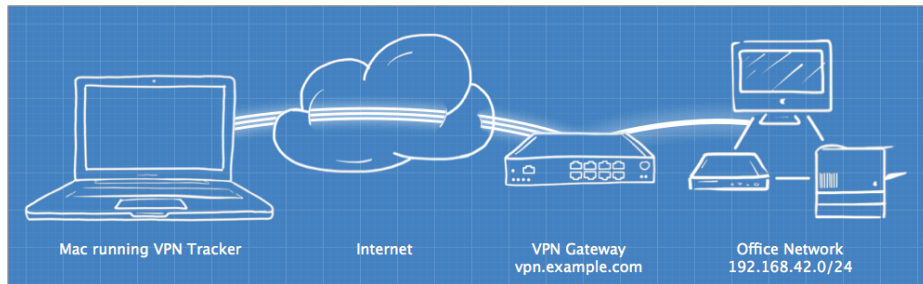
Getting Connected

VPN Crash Course

Is this your first time working with a VPN? Read this chapter to get you up to speed.

VP...What?

VPN Tracker allows your Mac to securely connect to another network over the Internet. Even if your office is located in San Francisco and you're on a business trip in New York, you can work with your applications and files, as if you were in your office.



How does it work?

As the name implies, VPN Tracker uses VPN (Virtual Private Network) technology to create a connection between your Mac and your remote network. And unlike normal Internet connections, a VPN Tracker connection is encrypted. Think of a VPN as a highly-secure tunnel through the Internet, your very own "secure line" to your office.

In order to use a VPN, you'll need your Mac running VPN Tracker on your end of the connection. On the other end of the connection (the remote side), you need a VPN gateway that accepts your incoming VPN connection.

Once you have set up your connection in VPN Tracker and on the device at your remote location, you are ready to connect and start working remotely using your normal tools and applications.

What do I need?

To create a VPN connection from your Mac, you need three things:

- ▶ VPN Tracker
- ▶ An Internet connection
- ▶ A VPN gateway

If you're reading this, you probably already have VPN Tracker and an Internet connection for your Mac. So what about a VPN gateway?

VPN Gateway

A VPN gateway is a hardware device (or in some cases specialized software running on a regular computer) that accepts incoming VPN connections, creating a secure tunnel between its local network and your Mac. In most cases, a VPN firewall or a router with built-in VPN capabilities will act as the VPN gateway.



If there are existing VPN users in your organization you probably already have a properly configured VPN gateway. If not, don't worry – check out the chapter on → *Choosing the Right VPN Device* for some tips on what to look for when buying a VPN gateway.

What kind of VPN connections does VPN Tracker support?

VPN Tracker supports industry standard IPsec VPN connections. IPsec VPN is fast, secure, and supported by a great variety of devices.

In addition, VPN Tracker Pro also integrates OS X L2TP VPN connections, as well as legacy PPTP connections. For more information, please refer to chapter → *L2TP / PPTP Connections*.

The Big Picture

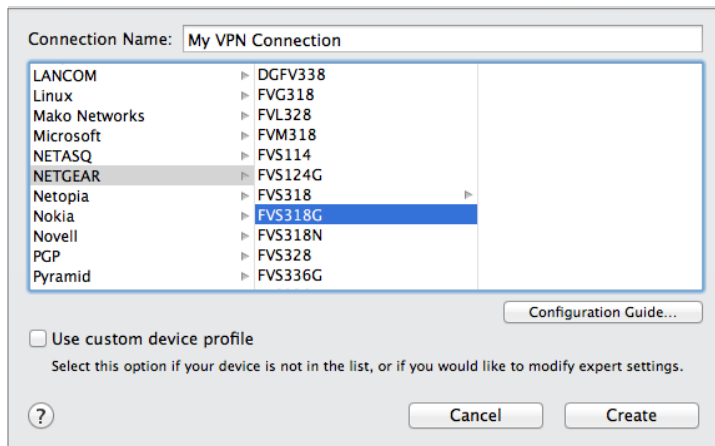
To give you a better idea how to set up your VPN, here's a quick overview. We'll look at the details in the following chapters, so don't worry about missing pieces right now – there will be a lot more specific information later on.

Add a New Connection

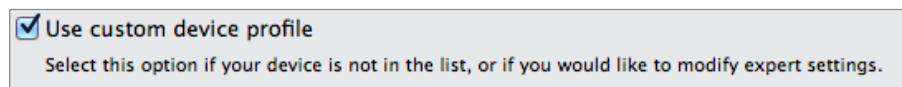
- ▶ Click the button in the lower left hand corner of the VPN Tracker window



You will see a list of device profiles. We have device profiles for all the VPN gateways that VPN Tracker has been tested with.



- ▶ Select your VPN gateway from the list. If your VPN gateway is not listed, check the box "Use custom device profile".



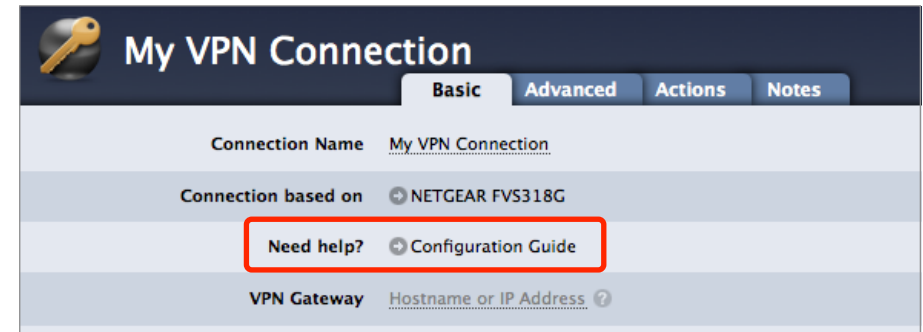
- ▶ Click "Create" to add the new connection

Find Your Configuration Guide

Our engineers have tested a large number of VPN gateways with VPN Tracker. For many of these, detailed configuration guides are available. Now is a good time to check whether a device-specific configuration guide is available.

In VPN Tracker

- ▶ Click "Configuration Guide" on the Basic tab.



- ▶ You will be taken to the configuration guide for your device, if available.

On the Web

All configuration guides are also available on our website:

<http://vpntracker.com/interop>



If a configuration guide is available for your device and you do not yet have VPN set up on your VPN gateway, you can go straight to the guide and follow it. Then continue with the chapters → *Secure Desktop* and → *Working with VPN Tracker* for more information on how to use your VPN connection.



VPN Tracker can also use L2TP or PPTP connections created by OS X. For more information, please see → *L2TP / PPTP*.

Basic Settings

Let's take a closer look at the essential settings that VPN Tracker needs to connect to your VPN gateway. Depending on your device, some settings may not be shown. If you don't know yet what to fill in, we'll cover each setting in detail later in this chapter.

Connection Icon

Customize the icon by dragging an image onto the default icon, or choose "Edit > Choose Image..." for a new icon.

Device Profile

Click to change the device profile.

VPN Gateway

Enter the public IP address or host name of your VPN gateway, e.g 203.0.113.48 or vpn.example.com

Authentication

Choose whether to use a pre-shared key, certificates or hybrid mode for authentication. Most VPN gateways use pre-shared keys.

Identifiers

Select the type and enter the local and remote identifiers.

Note: The identifiers need to be entered in reverse, e.g. "local" in VPN Tracker is what is configured as "remote" on your VPN gateway.

Connection Name

Click to change the name of your connection.

Configuration Guide

Click to access the device-specific configuration guide.

Network Configuration

Select manual configuration or one of the automatic configuration options (not available on all devices).

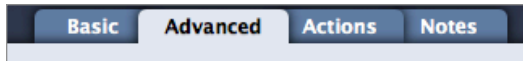
Extended Authentication

VPN Tracker will prompt you for username and password if your VPN gateway requests Extended Authentication (XAUTH).

DNS

VPN Tracker can use a DNS server on the remote network over VPN. It is not necessary to configure remote DNS right away, you can always do so later.

Advanced Settings



You likely won't have to modify any settings on the Advanced tab, unless:

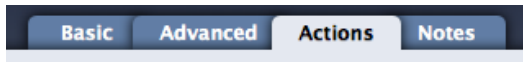
- ▶ your device uses different settings than the factory defaults and/or the settings proposed in the configuration guide, or
- ▶ there is no device profile for your device in VPN Tracker

In both cases, the goal is to have VPN Tracker's settings for Phase 1 and Phase 2 match exactly what is set up on your VPN gateway.



Some VPN gateways use different terms for phase 1 and 2: Phase 1 is sometimes called "IKE", while phase 2 may be called "VPN" or "IPsec". Check out the → *Settings Reference* for more details.

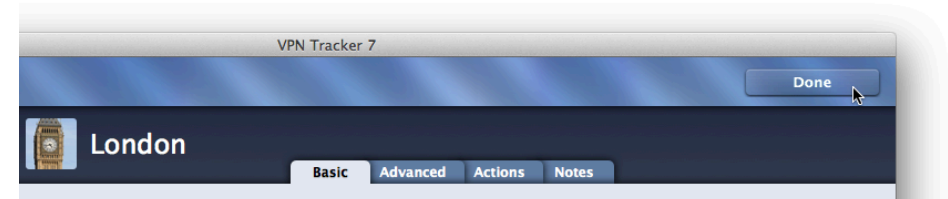
Actions and Notes



These settings are **not** relevant to VPN connectivity, so we will skip them for now. They are covered in detail in → *Working with VPN Tracker*.

Completing Setup

When you're done configuring your VPN, click the „Done“ button on the upper left corner to leave edit mode.



It is **not** necessary to leave edit mode to save the connection or to connect to the VPN. If you make changes while the VPN is connected, reconnect the VPN to apply them.

Now that you have a basic idea how to set up a connection in VPN Tracker, you're ready to apply it to your specific situation.

Are you connecting to a VPN that's already set up?

If you are connecting to an existing VPN (e.g. one that Windows users are already connecting to), all you need to do is gather a few pieces of information about your VPN gateway to configure VPN Tracker. The next chapter → *Setup for an Existing VPN* has all the details.

Are you setting up both your VPN gateway and VPN Tracker?

Check if your VPN gateway has been tested with VPN Tracker and if there is a configuration guide available (see → *Find Your Configuration Guide*).

- ▶ If a configuration guide is available, follow it.
- ▶ If no configuration guide is available for your device, or if you are working with an untested device, → *Setup without Configuration Guide* will help you get connected.

Did you receive a VPN Tracker connection from your administrator?

Follow → *Importing Connections* to see how to use the connection in VPN Tracker.

Setup for an Existing VPN

When connecting to a VPN that's already set up, your goal is to configure VPN Tracker to match the settings on your VPN gateway. In order to do so, you will need information about the VPN gateway's configuration.

What if my organization does not support Macs?

We often hear from customers in organizations where Macs are not officially supported for VPN access. It may be difficult to get help if the IT help desk isn't set up to support Mac users. We're here to help!

To find out more about your VPN gateway's configuration, your first stop should be your VPN gateway's administrator: Your network administrator, your IT department or your help desk are good places to ask.

If they cannot help, you may be able to obtain the settings from another VPN client that has already been configured, for example on a Windows PC.

Obtain the Configuration

You will always need the following information:

- ▶ The public IP address or host name (e.g. "203.0.113.48" or "vpn.example.com") of the VPN gateway you are connecting to
- ▶ The brand of the VPN gateway (e.g. Cisco, SonicWALL, NETGEAR, ...)
- ▶ The pre-shared key¹ or the client certificate

You may also need one or more of the following:

- ▶ The address of the network you are connecting to through VPN
- ▶ The local identifier²
- ▶ The model name of the VPN gateway (e.g. ASA Series, TZ Series, FVS318N, ...)
- ▶ The settings for phase 1 and 2 (encryption algorithms etc.)
- ▶ Your username and password, if Extended Authentication (XAUTH) is used

¹ Not required for SonicWALL with "Use Default Key for Simple Client Provisioning" enabled

² Some VPN gateways (e.g. Cisco) refer to the local identifier as "group name" or "group ID"



If you have any questions about specific settings, please refer to the → *Settings Reference* in this manual. For some settings, in particular phase 1 and 2 algorithms, it may be possible to "guess" them – the reference will tell you if and how.

Cisco IPsec VPN

If you have a Cisco IPsec VPN connection profile (.pcf), you can import it directly into VPN Tracker (File > Import > Cisco VPN Client Connection).

Configure VPN Tracker

- ▶ Create a new VPN connection if you have not yet done so (see → *Add a New Connection* for additional information).
- ▶ Enter the settings you obtained in the Basic and Advanced tabs.



If there is a configuration guide for your VPN gateway (→ *Find Your Configuration Guide*), refer to it for additional advice. Keep in mind that the configuration guide describes a working setup, but not the only working setup. **In most cases, you won't need to make changes to a working setup on the VPN gateway.**

Connecting

When you're done setting up, skip ahead to → *Connecting to Your New VPN* to see how to connect to your new VPN.

Setup without Configuration Guide

Almost all IPsec VPN gateways can be used with VPN Tracker, even if they have not been tested with VPN Tracker.

Set up Your VPN Gateway

Network Setup

If you haven't already done so, set up your VPN gateway so it is connected to the Internet and to the internal network that you want to access using VPN Tracker. Please refer to your VPN gateway's manual for more information on how to do this.



It is a good idea to carefully choose the address of the VPN gateway's LAN network if you plan to access it through VPN. To avoid address conflicts, use a private network that is not used very frequently (e.g. 192.168.142.0/24, or 10.42.23.0/24).

VPN Setup

Once you have completed the initial setup of your VPN gateway, it is time to configure VPN on the VPN gateway. Go for the simplest possible configuration first. You can always move to a more sophisticated setup later.

If your VPN gateway's manual has instructions for setting up a VPN connection, follow it. Otherwise, please follow these basic settings as closely as possible:

Authentication

- ▶ Choose **pre-shared key authentication**.
- ▶ For now, use a pre-shared key that is not too complex to avoid typos. But don't forget to change it to a very strong password later!

Aggressive Mode vs. Main Mode

- ▶ For most devices, you should use **Aggressive Mode** for now.

- ▶ **Main Mode** is considered more secure, but may not work with all devices for clients connecting from dynamic IP addresses. You can try Main Mode once you've got everything else working.

Identifiers

- ▶ Choose **Fully-Qualified Domain Name (FQDN) identifiers**, if possible.
- ▶ With most devices, you can enter any identifier you want, it doesn't have to be a valid domain name. Good choices would be:
 - Local identifier: `vpngateway.local`
 - Remote identifier: `vpntracker.local`
(the remote identifier is sometimes called "peer identifier")
- ▶ Some devices use the group name as the remote identifier.

Proposals (Phase 1 and 2 Settings)

- ▶ **Encryption algorithms:** AES-128 or 3DES
- ▶ **Hash/Authentication algorithms:** SHA-1
- ▶ **Diffie-Hellman (DH) group 2 (1024 bit)**
- ▶ Enable **Perfect Forward Secrecy (PFS)** using **DH group 2 (1024 bit)**

While these are not the most secure settings, they are compatible with a wide variety of devices. Use them as a starting point. Once you've got the VPN working, switch to stronger algorithms if available (e.g. AES-256, SHA-2, DH group 5 or higher).

Local Endpoint (Network Access / Policy)

- ▶ On most VPN gateways, you will have to configure the network(s) VPN users can access. This setting is often called "**local endpoint**", or "**policy**".
- ▶ Enter the address of the network you would like to access. Usually this will be the same as the VPN gateway's LAN network (e.g. 192.168.142.0/24).
- ▶ This setting will later be configured in VPN Tracker as the Remote Network.

Remote Endpoint

- ▶ Some VPN gateways will also ask you to configure the "**remote endpoint**" of the VPN. The remote endpoint is the address VPN clients will be using when connected through VPN.
- ▶ Whenever possible, set this to "any address" or "dynamic" (sometimes also referred to as "0.0.0.0/0").

- ▶ If your VPN gateway requires a single address to be entered, this will mean that only one VPN client can use this VPN connection at a time. It also means that you will have to take the address you configure on the VPN gateway, and enter it in VPN Tracker as the Local Address.

VPN Gateway IP Address or Hostname

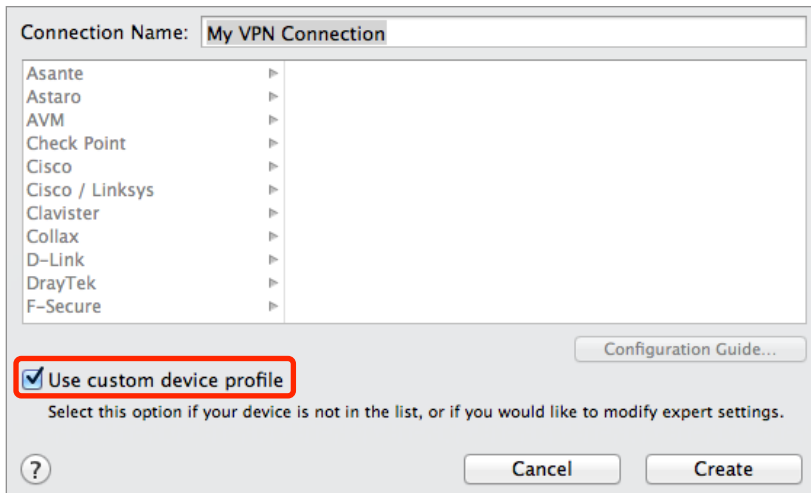
- ▶ Finally, write down your **VPN gateway's public (WAN) IP address** or host name.
- ▶ If your VPN gateway's public IP address is dynamic, you might want sign up with a dynamic DNS service so you can always refer to it by host name.



If any other settings are required by your VPN gateway to set up a basic VPN connection, check the → *Settings Reference* in this manual and your VPN gateway's documentation for more information on what to configure.

Configure VPN Tracker

Once you have your VPN gateway set up, enter the settings in VPN Tracker. For your connection, use a custom device profile to have access to all settings.



The screenshot shows a configuration dialog box for a VPN connection. At the top, the "Connection Name" field is filled with "My VPN Connection". Below this is a list of device profiles with right-pointing arrows next to each name: Asante, Astaro, AVM, Check Point, Cisco, Cisco / Linksys, Clavister, Collax, D-Link, DrayTek, and F-Secure. At the bottom of the dialog, there is a checkbox labeled "Use custom device profile" which is checked and highlighted with a red rectangle. Below the checkbox is the text: "Select this option if your device is not in the list, or if you would like to modify expert settings." To the right of the checkbox is a button labeled "Configuration Guide...". At the bottom left is a help icon (a question mark in a circle). At the bottom right are two buttons: "Cancel" and "Create".

Then enter your settings. Please refer to → *Getting Connected* to see where required settings are located. Also check the → *Setting Reference* if you are unsure about a specific setting.

A few final notes:

- ▶ The identifiers are swapped in VPN Tracker. What is **local** from the VPN gateway's perspective, is **remote** from VPN Tracker's perspective, and vice versa. You can set the remote identifier to "Don't verify remote identifier" so you don't have to deal with it for now.
- ▶ If you were able to select the algorithms and Diffie-Hellman (DH) groups suggested earlier, you do not have to modify any setting on the Advanced tab. However, if the suggested settings were not available on your device, make sure to customize the phase 1 and 2 settings on the Advanced tab so they match what is configured on your VPN gateway.

Connecting

When you're done setting up, skip ahead to → *Connecting to Your New VPN* to see how to connect to your new VPN.

Importing Connections

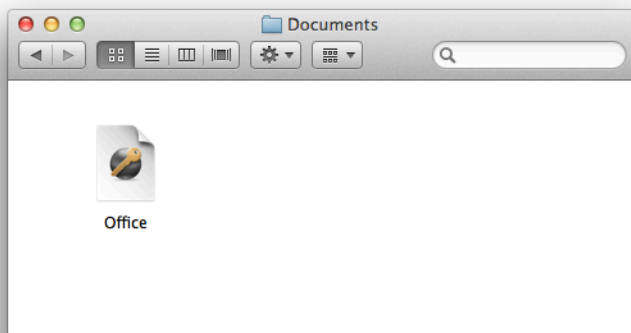
Find out how to import a connection that you have been given by your IT department or VPN administrator.

Prerequisites

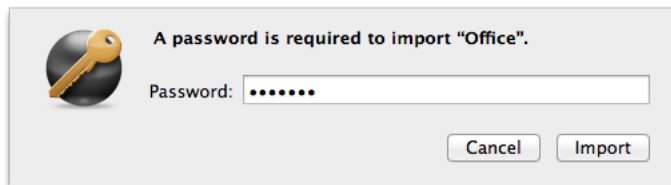
Before importing a connection, make sure VPN Tracker is installed. If you have not yet downloaded or installed VPN Tracker, or if you haven't activated your license yet, please follow → *Getting Started* first.

Import Your Connection(s)

- ▶ Locate the connection in Finder and double-click it. Or open VPN Tracker and choose "File > Import > VPN Tracker Connection..." from the menu.

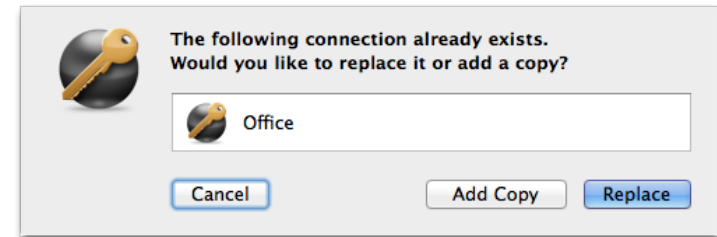


- ▶ You will be asked for the import password. If you don't know the import password, please ask the person who gave you the connection.



Replacing Existing Connections

If you already have the connection you're about to import, you'll be asked whether to replace your existing connection, or if you would prefer to add this connection as a copy:



Replacing a connection

If your new connection replaces your existing connection, click "Replace". Your existing connection will be overwritten.



Adding a copy

If you would prefer to keep your existing connection and import the new copy, click "Add Copy".

You'll find the imported connection further down in your connection list. It will have the word "copy" appended to its name, e.g. "Office copy".

Replacing an Existing Secure Desktop

Connection files can also include Secure Desktops. If the included Secure Desktop already exists, you will once again be asked whether you would prefer to replace your existing Secure Desktop or add a the new Secure Desktop as a copy.

Connecting to Your New VPN

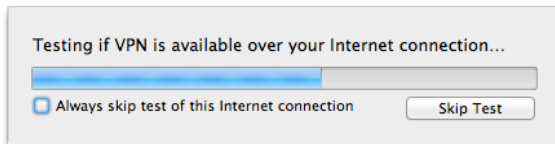
When you're done setting up your VPN, you're ready to connect. To test your VPN, go to a location outside of the network that you want to connect to.

Connecting

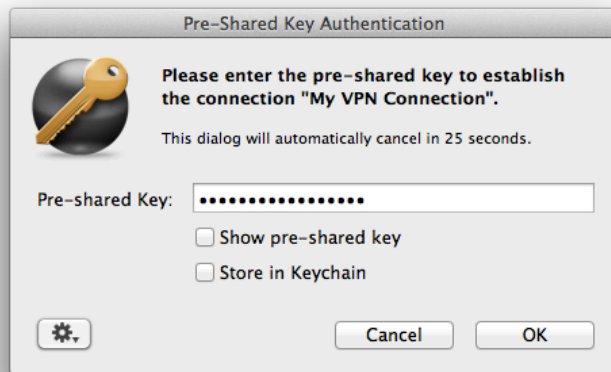
Click the on/off slider to connect the VPN.



If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.

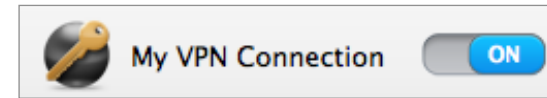


If prompted, enter your pre-shared key and Extended Authentication (XAUTH) user name and password.



Connected?

Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected!

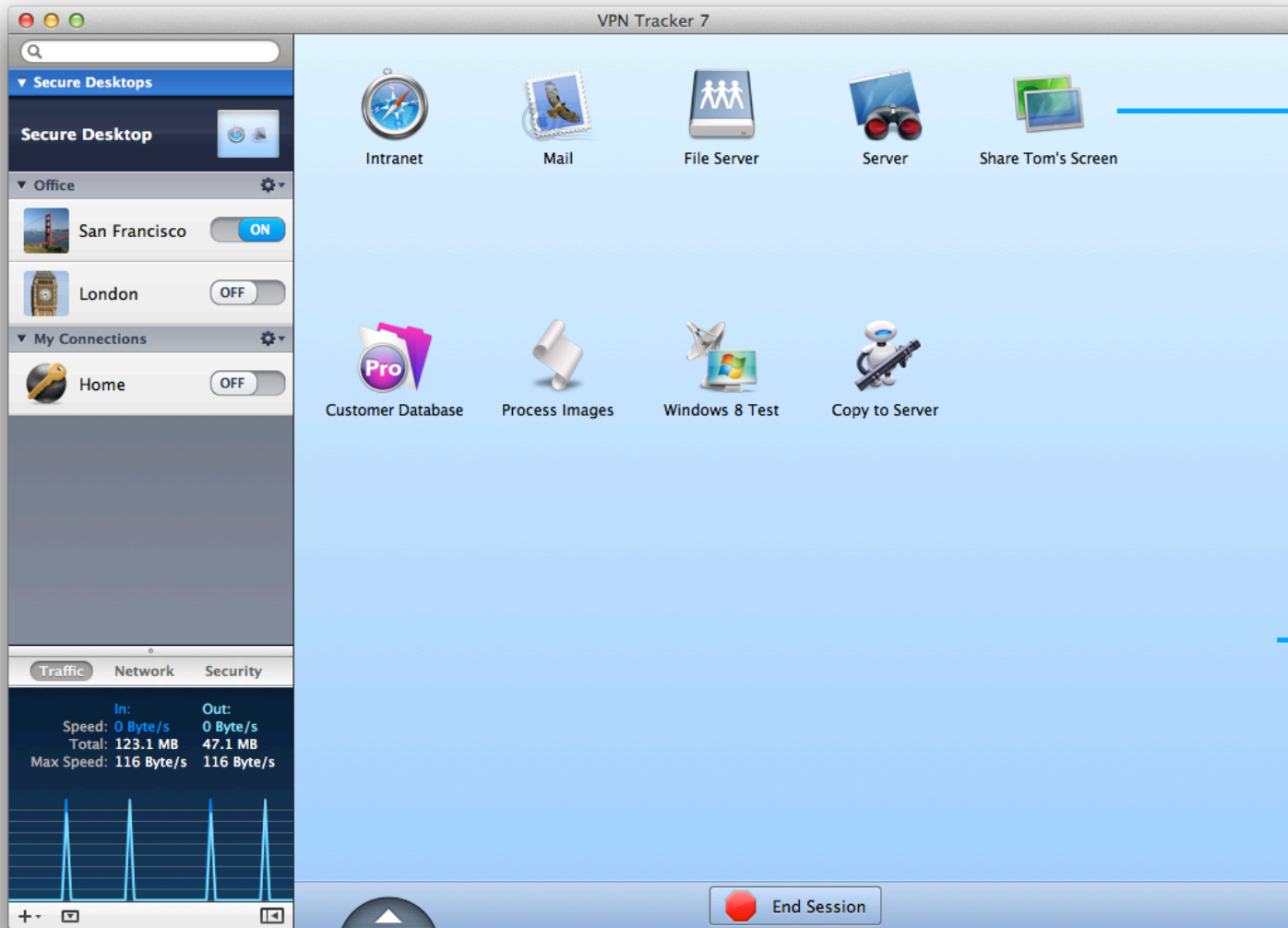


Continue with the chapters → *Secure Desktop* and → *Working with VPN Tracker* to find out how to use your VPN connection.

Problems?

If there is a problem connecting, VPN Tracker will give you helpful advice and troubleshooting tips. To learn more about troubleshooting VPN connections, visit the chapter → *Troubleshooting*

Working with VPN Tracker



Secure Desktop Items

Click an icon to launch an application, connect to a server etc.

VPN Tracker will automatically take care of connecting your VPN.

Secure Desktop Background

Drag in a picture while in edit mode, to give your Secure Desktop a personal touch. Or choose any color you like.

Edit your Secure Desktop

Click the triangle to drag new items to your Secure Desktop, and edit existing ones.

End Session

When you're done working over VPN, click the "End Session" button to take care of closing and disconnecting everything.

Secure Desktop: Your VPN Cockpit

Connect to file servers, launch the applications you need, and much more. And stop thinking about VPN connections.

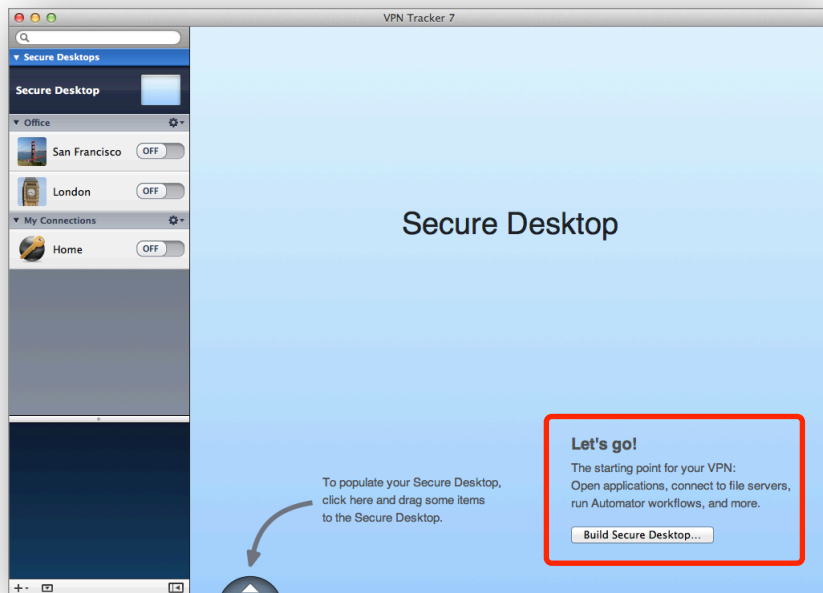
Setting up your Secure Desktop

Working over a VPN connection used to be a hassle. First you needed to connect to your VPN. Then you went to Finder in order to connect to your file servers, and finally, you could open the applications you need and get to work.

Not any more! VPN Tracker is designed with your workflow in mind: You click to open the application. VPN Tracker does the rest.

Building your Secure Desktop with the Assistant

To add items to your Secure Desktop, select it from the top left corner of the VPN Tracker window and then click "Build Secure Desktop".



VPN Tracker will guide you through selecting applications, file servers and websites for your Secure Desktop. Of course you can always modify your Secure Desktop later, so don't worry if you don't yet know what to add.



Make sure you have set up your VPN connection first. To learn how to set up your VPN connection, refer to the chapter → *Getting Connected*.

Adding Applications to Your Secure Desktop

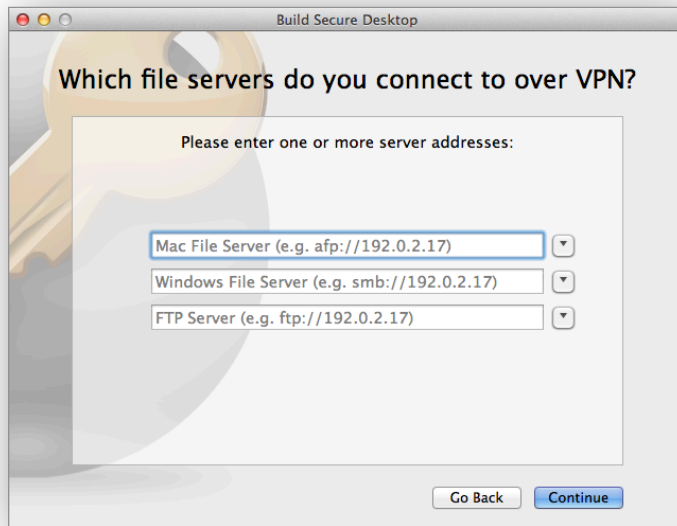
The Secure Desktop Assistant will suggest a few commonly used applications. If your application is not among them, click "Other Application..." to add the application you want to use.



You can also add applications to your Secure Desktop later, so don't worry about them now if you're not sure.

Adding File Servers to Your Secure Desktop

If you would like to access a file server, enter the details in the Secure Desktop Assistant.



To connect to a Mac-based (AFP) file server:

- ▶ Enter "afp://" followed by the IP address¹ of the server, e.g. afp://192.168.144.11

To connect to a Windows-based (SMB) server:

- ▶ Enter "smb://" followed by the IP address¹ of the server, e.g. smb://192.168.144.17

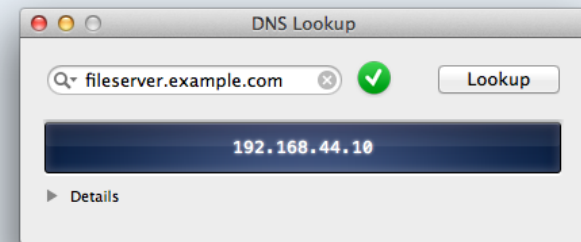


Alternatively, you can connect to file servers in the OS X Finder. → *Accessing Files, Printers and Databases* has more details. For more information about file servers in Secure Desktop, take a look at the → *Secure Desktop Reference*

I don't know my file server's IP address. Can't I just browse for my file servers via the Finder Sidebar?

For technical reasons, when using a VPN connection, your servers won't show up in the Finder sidebar. If you don't have your file server's IP address, you can easily find it out next time you're in your office network (or whatever other network you're connecting to through VPN):

- ▶ Open "Tools > DNS Lookup..."
- ▶ Enter your file server's name and click "Lookup"



After a few seconds, VPN Tracker should tell you the file server's IP address. Again, this will only work when you're actually in your remote network, not if you're connected via VPN.

Adding Websites to Your Secure Desktop

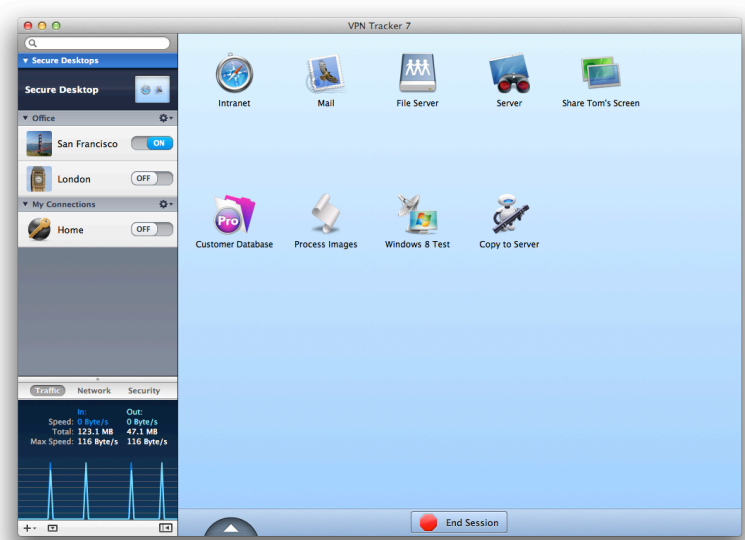
If you have intranet websites that you need to access over VPN, you can add those to your Secure Desktop as well. Just enter your website URLs when prompted by the Secure Desktop Assistant.

Customizing Your Secure Desktop

If you would like, you can customize the name and color of your Secure Desktop. Then click to finish creating your new Secure Desktop.

¹ If your connection is set up to use remote DNS, you may also be able to enter a DNS host name, e.g. "fileserver.example.com"

Working with Secure Desktop



Starting a Secure Desktop Session

Click one of the icons on your Secure Desktop to start working with that application, file server or website. VPN Tracker will automatically connect any necessary VPN connections, and then open your application, connect to your file server, website, etc.



To use Secure Desktop when your Mac is physically connected to your VPN's remote network (e.g. at the office), teach VPN Tracker to recognize your remote network using → *Direct Link Detection*.

Ending a Secure Desktop Session

Once you're done working over VPN, simply end your session by clicking the large red button at the bottom of the window. VPN Tracker will take care of disconnecting file servers and disconnecting your VPN.

Multiple Secure Desktops

You can have more than one Secure Desktop (e.g. for different clients, departments or tasks). To add a new Secure Desktop, choose File > New Secure Desktop from the menu bar on top of your screen.

Editing Your Secure Desktop

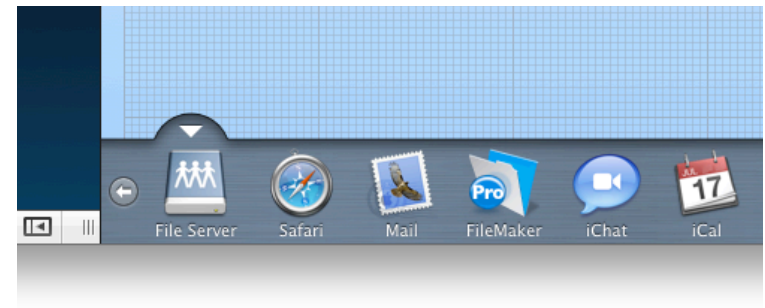
You can easily add, modify or remove Secure Desktop items.

To edit your Secure Desktop:


- ▶ Select the Secure Desktop that you would like to edit.
- ▶ Click the triangle at the bottom to switch to edit mode



- ▶ A drawer with new items will open. Drag an item to your Secure Desktop to add it. Or drag an existing item outside your Secure Desktop to remove it.



appletree.example.com



VNC (Virtual Network Computing)
TCP Port: 5900

Connect... →

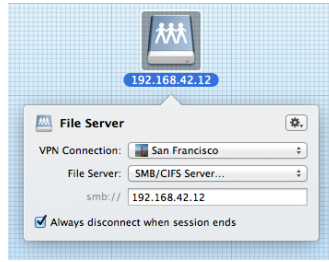
Adding Items from the Network Scanner PRO

You can add new items to your Secure Desktop right from the Network Scanner!

Just click the arrow button and choose "Add to Secure Desktop", or drag the services straight to a Secure Desktop in the sidebar.

To modify an item, click it while Secure Desktop is in edit mode. To finish editing, click on a free space on your Secure Desktop or hit the Esc key.

When you are done configuring, click the triangle again to leave the edit mode.



Customize the Appearance of Your Secure Desktop

You can give your Secure Desktop a personal touch, by adding your own picture, choosing your own background and changing icons.

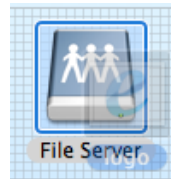
To customize your Secure Desktop icon:

VPN Tracker automatically shows a preview of what's on your Secure Desktop. If you wish, you can replace that with a custom icon, simply drag the new icon onto the preview in the sidebar.



To customize the icons of your Secure Desktop items:

- ▶ Switch Secure Desktop to edit mode by clicking the triangle
- ▶ Drag an image onto one of your Secure Desktop icons



To customize your Secure Desktop background

- ▶ Switch the Secure Desktop to edit mode by clicking the triangle
- ▶ Drag an image to your Secure Desktop

or

- ▶ Right-click or Ctrl-click the Secure Desktop area
- ▶ Select a background image or background color
- ▶ Enjoy the view!



Further information about Secure Desktop is available in the → *Secure Desktop Reference*.

VPN Productivity

Find out about other VPN Tracker features that will help you work more productively with your VPN.

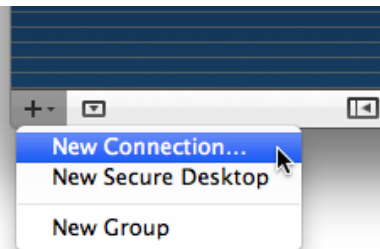
Managing Connections and Secure Desktops

At this point, you probably already have your first VPN Tracker connection. You can see your connection in the sidebar on the left-hand side of the VPN Tracker window.

Adding More Connections or Secure Desktops

To create a new connection or Secure Desktop, click the '+' icon in the lower left hand corner of the window.

For more information on setting up a new connection, please refer to the → *Getting Connected* chapter.



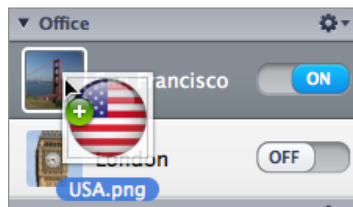
Reordering

Drag & drop your connections and Secure Desktops in the sidebar to reorder.

Renaming

To rename connection or Secure Desktop, right-click (or hold down Ctrl and click) it in the sidebar and select „Rename“ from the menu.

Icons



To customize the icon for a connection or a Secure Desktop, drag the new image onto the existing icon in the sidebar.

You can also use „Edit > Choose Icon...“ in the menu to change icons.

Locking Connections

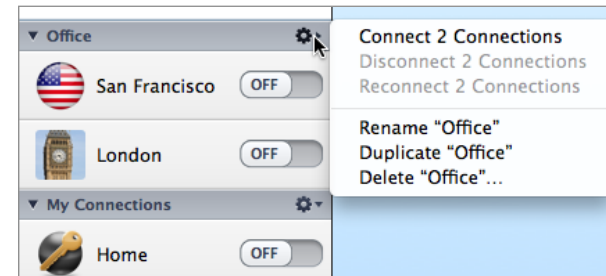
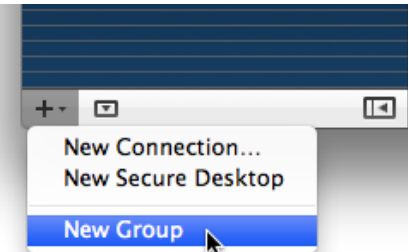
You can lock a connection with a password to prevent it from being modified (VPN > Lock Connection...). To prevent others from modifying connections you export for them, enable locking in the export settings.

Organizing Connections in Groups **PRO**

If you have a lot of connections, it will be useful to divide your connections up into groups, e.g. by client, by branch office, by geographical location etc.

To add a new group, click the '+' icon in the lower left hand corner of the window and select 'New Group'.

You can drag & drop connections and Secure Desktops between groups to rearrange them.



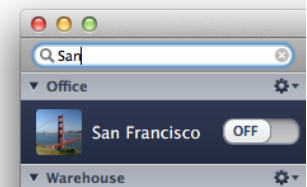
To rename, delete or control a group of connections, use the gear menu on the right side of the group.



An exported connection knows the group it belongs to, and will recreate it as needed.

Search **PRO**

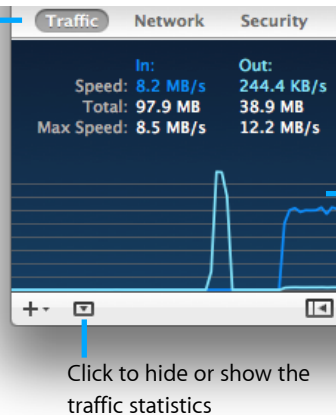
If you are looking for a specific connection, use the search box at the top of the sidebar to find it.



VPN Connection Stats

When connected to your VPN, you can see statistics for your connection in the sidebar. The traffic graph lets you know how much data is currently being sent and received over your VPN connection, the total amounts of data transferred, and the maximum throughput seen in the last measurement period. It also lists the the algorithms that are in use and the current network settings.

Click to toggle between traffic, network or security information



The graph indicates the amount of traffic currently being transferred over the VPN connection

Click to hide or show the traffic statistics

Hide the Details

If you only want to see your connections and the connection status, you can hide the entire right part (the connection details) of your VPN Tracker window.

To hide or show the connection details:

- ▶ Click the details toggle at the bottom of the connection list



Click to hide or show the connection details.

Menu Bar Item

You can also control VPN Tracker directly from your menu bar, allowing you full control over your VPN connection, without having to leave the application you're working in.

The stop button will disconnect any file servers and end all VPN connections.

The key in menu bar icon will turn black, when you're connected.

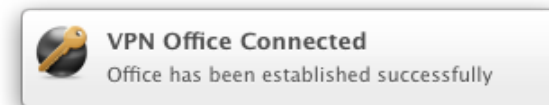
Access your Secure Desktop items from the menu bar.

Click to start or stop a connection. Check mark indicate established connections.



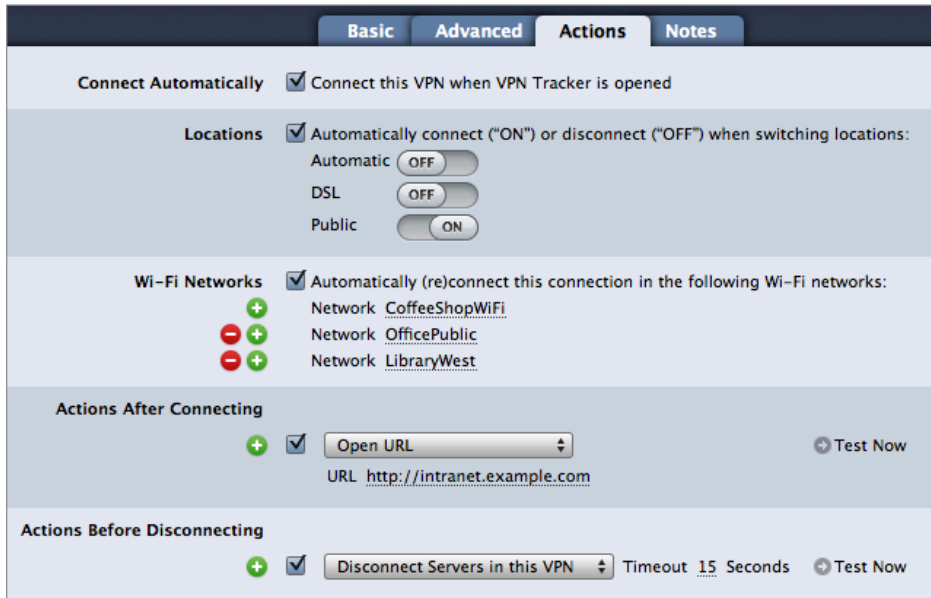
Notifications

VPN Tracker shows little popup notifications whenever something interesting happens to your VPN.



You may customize these notifications in "VPN Tracker 7 > Preferences..."

Actions



Connect this VPN when VPN Tracker is opened

Enable this option to automatically connect to this VPN whenever VPN Tracker is opened.

Locations

If you use multiple network locations on your Mac (System Preferences > Network), VPN Tracker can automatically connect or disconnect your VPN connection, depending on the current network location.

- ▶ Switch the slider to "On" to automatically connect in this location
- ▶ Switch the slider to "Off" to automatically disconnect in this location

Wi-Fi Networks

VPN Tracker will automatically connect to your VPN whenever your Mac connects to the wireless networks you have specified.

Actions after Connecting

VPN Tracker can take care of any tasks that need to be performed after the VPN connects.

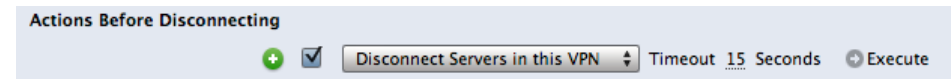
For example, if you always need to connect to a file server, enter it here to make sure it's available any time you connect the VPN. Or if you want to open your company's intranet website whenever you connect, enter it here.



Actions can help you to be even more productive with Secure Desktop. For example, if you have certain applications on your Secure Desktop that require a file server to be connected, add that file server here to ensure that it's always available to your Secure Desktop items.

Actions after Disconnecting

If there's anything that needs to be taken care of before the VPN is disconnected, add it here. VPN Tracker automatically adds an action to disconnect all file servers that use the VPN.



Actions that can take a long time have a timeout to make sure VPN Tracker does not keep trying forever.



Actions can also be AppleScript or shell scripts. There is no limit to what you can do!

Notes

Basic		Advanced		Actions		Notes	
Organization	Example Inc.						
Reference #	A790D2						
Contact	John						
Email	john@example.com						
Phone	555-345823						
Website	http://intranet.example.com/helpdesk						
Notes	VPN Access may be unavailable during maintenance hours (Friday 8 to 10 PST)						

If you would like to make a few notes – for yourself, or for others that you’re setting up this VPN for, the Notes tab is the right place.

- ▶ Notes are included with exported connections
- ▶ When exporting Accounting records, the reference number and organization can be included for use with billing systems
- ▶ All information from the Notes tab is displayed on the Status tab

The diagram illustrates a network setup for a VPN connection. On the left, a laptop labeled 'This Mac' with IP address 192.168.213.189 is connected to a cloud labeled 'Internet'. The 'Internet' cloud is connected to a 'VPN Gateway SonicWALL TZ 210' with IP address 194.145.236.73 and domain vpntest.equinux.net. The VPN Gateway is connected to a 'Remote Network' with IP address 192.168.213.0/24. Below the diagram, there are two buttons with right-pointing arrows.

Organization	Example Inc.	Notes	VPN access may be unavailable during maintenance hours (Friday 8 to 10 pm PST)
Reference #	6195A10		
Contact	John		
Email	john@example.com		
Phone	555-737120		
Website	http://www.example.com/helpdesk		

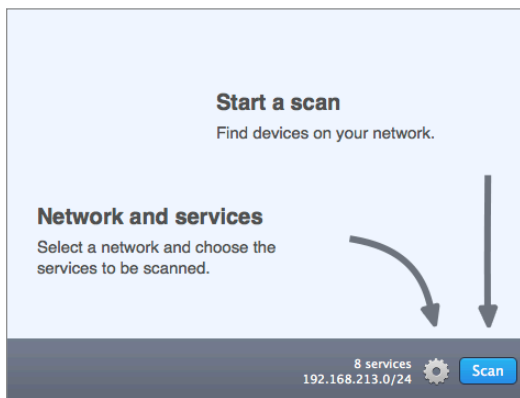
Network Scanner **PRO**

The Network Scanner in VPN Tracker Pro lets you explore the remote network of your VPN, assist users and easily locate hosts and services.

Scanning Networks

To scan a network, your Mac must be connected to the network via VPN.

- ▶ Select the VPN in the sidebar and connect the VPN.
- ▶ Open the Scanner tab.
- ▶ Click the Scan button to scan the network using a selection of the most popular network services.



If you are connected to a VPN where all network traffic is sent through the VPN (Host to Everywhere), VPN Tracker will ask you to specify the network that you would like to scan.

Depending on the size of the network and your Internet connection, the scan may take a while to complete. You can continue working with VPN Tracker while a scan is in progress. You'll see a notification when the scan is complete.

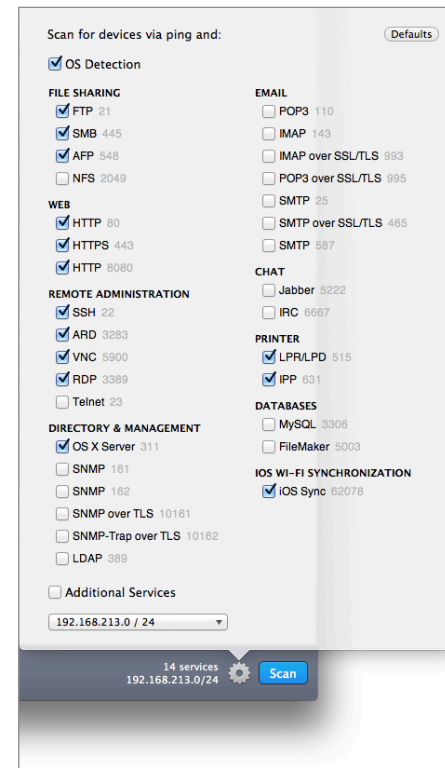


To be able to use the Network Scanner when you're physically at the remote network and no VPN is needed, set up → *Direct Link Detection* for your VPN connection.

Customizing Network and Services

By default, the Network Scanner scans for a selection of the most popular network services.

- ▶ To select different services, click the gear icon and check or uncheck the services that you would like VPN Tracker to scan.
- ▶ To turn OS detection on or off, use the checkbox at the top of the settings.
- ▶ To check/uncheck all services, hold down the Option key while clicking a checkbox.
- ▶ To restore the default selection of services and networks, click the "Defaults" button at the top of the settings.

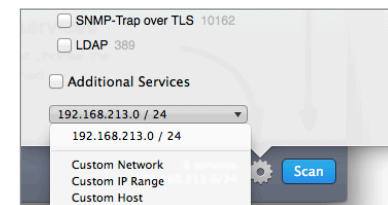


OS Detection

The Network Scanner can detect the type of host (e.g. OS X, Windows, Linux, Network Equipment, Printers) from the services that are available on that host.

OS detection requires certain services to be included in the scan. If you uncheck a service that is required for OS detection, OS detection will be unchecked as well.

At the bottom of the settings, you can change the network that is being scanned. Select one of the remote networks of the VPN, or enter a custom range or IP address. The more addresses a scan includes, the longer it will take.



Scan Results

Display Mode

Show results by address (IP address or host name) or by service.

Web Previews

A preview is automatically generated for web servers so you can easily recognize different web servers.

Filter Results

Type a search term to locate specific hosts or services. Use the popup button to show or hide groups of hosts or services.

Your Mac

If your Mac was part of the scan, it is marked with a home icon.

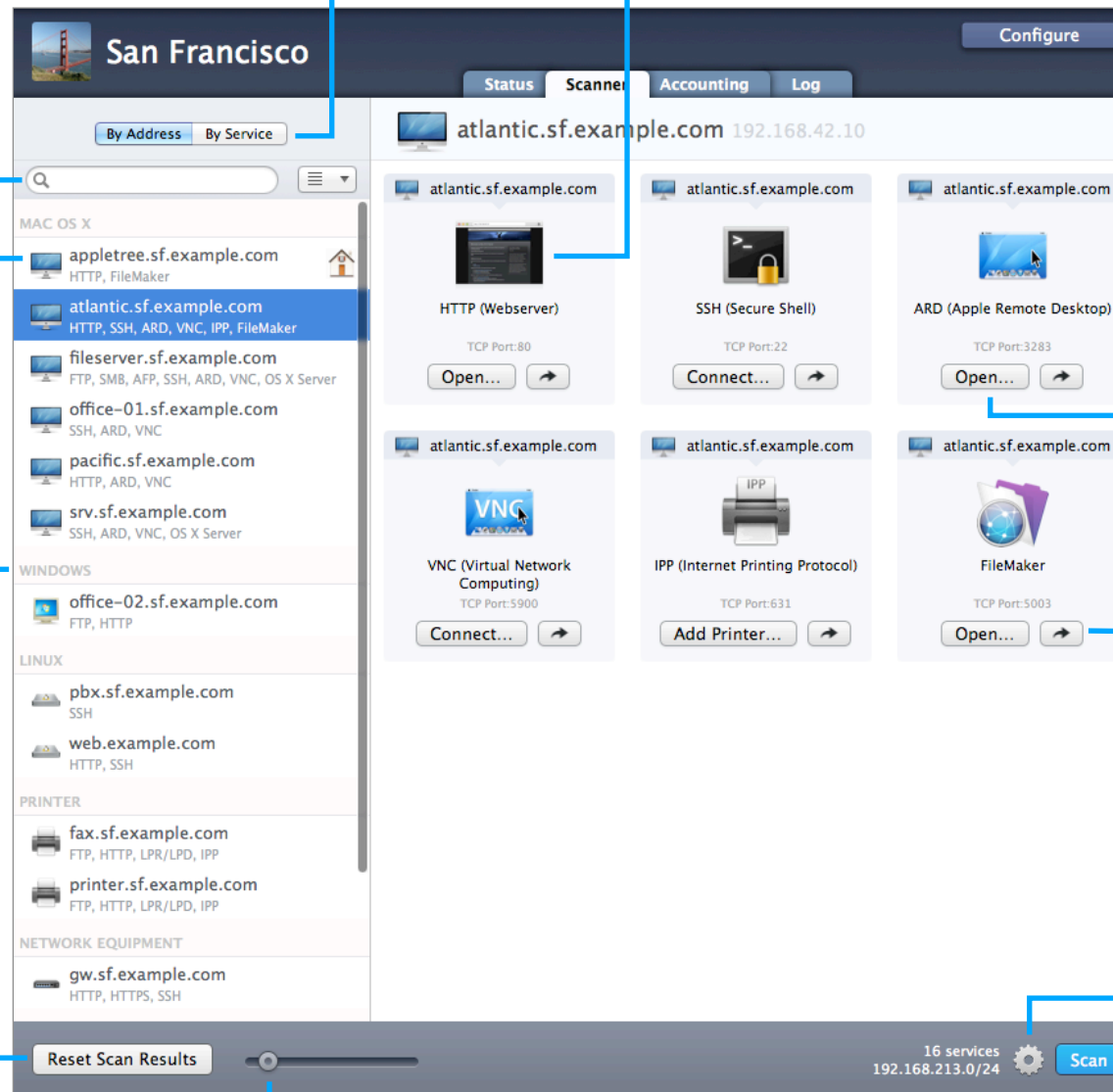
OS Detection Group

If OS detection is enabled, hosts are grouped according to the OS that was detected (the detected OS can change during the scan as more results come in).

Reset Scan Results

Click to remove all scan results.

If you hold down the Option key while clicking, your customizations (names, icons, groups) will also be removed.



Services / Hosts

The right side of the window displays the services for the selected host ("By Host") or the hosts for the selected service ("By Service")

Instant Connect

Click to connect to the service or open the application associated with this service on your Mac.

Go Button

Click to add the service to Secure Desktop, copy IP addresses, or jump to all services of this kind or host.

Settings

Click to select the services to scan or change the IP range that is being scanned.

Size Slider

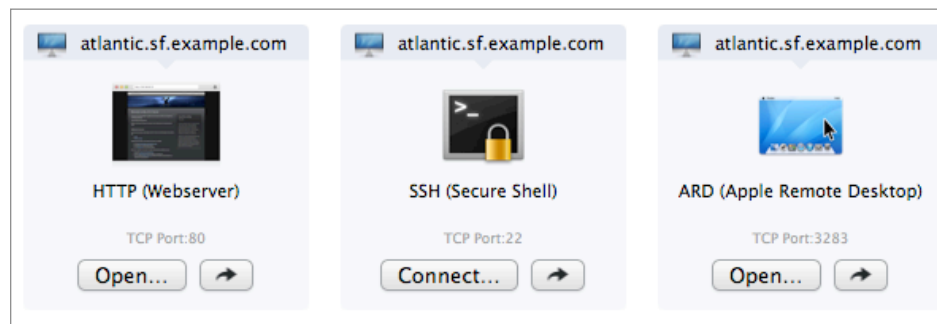
Drag to change the size of icons and web previews.

Using Scan Results


Connect to Services

You can connect to a service right from the Network Scanner, or open the app associated with this service on your Mac.

- ▶ Display the scan results "By Address" or "By Service"
- ▶ On the right side, click the "Connect" or "Open" for the service or host that you would like to connect to.



Add to Secure Desktop

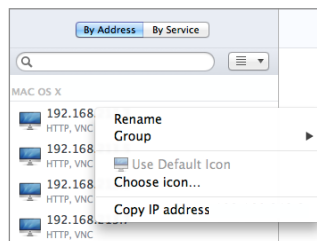
- ▶ To add a service to Secure Desktop, click the  button for the service that you would like to add to Secure Desktop.
- ▶ Choose "Add to Secure Desktop" and select the Secure Desktop that you want the service to be added to.
- ▶ You can also drag a service to your Secure Desktop in the sidebar.

Customizing Scan Results

Renaming Hosts

Renaming hosts in the Network Scanner list makes it easy to locate your most important computers and network devices.

- ▶ Display the scan results "By Address"
- ▶ Right click the host you want to rename.
- ▶ Choose "Rename" and enter a name.



Automatic Hostname Lookup

VPN Tracker can automatically look up the host names for IP addresses in the Network Scanner. All you need is a → *Remote DNS* server for your VPN that can provide host names for the IP addresses that are being scanned (reverse DNS lookup). Make sure the checkbox "Use for reverse lookup of IP addresses in remote networks" (Basic > DNS) is checked.

Setting a Custom Icon for a Host

- ▶ Display the scan results "By Address"
- ▶ Right click the host you want to change the icon for.
- ▶ Click "Choose Icon..." to set a custom icon for this host.

Change the OS Detection Group

The Network Scanner can automatically detect the kind of host – whether it's a Mac running OS X, a PC running Windows or Linux, or a printer or network equipment. OS detection uses the services on a host to determine the most likely type of host.

In some cases, OS detection might put a host into a different group than what it actually is. You can change the group if a host is not detected correctly.

- ▶ Display the scan results "By Address"
- ▶ Right click the host whose group you want to change.
- ▶ Select the new group from the "Group" menu.

Resetting Scan Results

- ▶ Click "Reset Scan Results" in order to clear the results. Customized host names, icons, and groups will not be modified – if the host is encountered again in a future scan, the customization will be applied.
- ▶ Hold down the Option key while clicking "Reset Scan Results" in order to also reset all customization (names, icons, and groups).

Scanner Preferences

You can configure the Network Scanner's performance and aggressiveness, and enable or disable Web Preview loading in → *Scanner Preferences*.

Accounting PRO

Accounting tracks the time you were connected to your VPN. It can assist you with billing your clients, documenting your work, or figuring out 6 weeks later when exactly you logged in to make that configuration change.

Customize the Display

- ▶ To select the month for which data is being displayed, click the back/forward buttons next to the month.
- ▶ To select the columns displayed in the Accounting table, right-click the table header and check or uncheck the columns.

Add Comments

You can add a comment for every connection to your client's VPN. This helps you to keep track why you used the connection on this day and also makes billing easier. To add a comment, double-click the "Comment" field.

Date ^	Weekday	Duration	Duration rounded	Local IP	VPN Gateway IP	Traffic	In	Out	Comment
Today 3:40 PM	Monday	1 h 07 min	1.25 h	192.168.213.62	194.145.236.73	1.00 MB	0.43 MB	0.57 MB	setting up
Today 2:13 PM	Monday	11 sec	0.25 h	192.168.213.189	194.145.236.73	25.52 kB	24.84 kB	0.68 kB	
Today 2:13 PM	Monday	27 sec	0.25 h	192.168.213.189	194.145.236.73	0.48 MB	0.27 MB	0.21 MB	

Exporting Accounting Data

VPN Tracker Pro not just tracks connection time for you, it also lets you export it for Numbers or Excel, or to third-party time tracking or billing systems that can import CSV files.

- ▶ Click "Export" in the "Accounting" tab
 - ▶ Choose "Export for Numbers..." or "Export for Excel..." depending on with which application you want to use the data with
 - ▶ To export data in a customizable CSV format, choose "Custom Export..."
- The export can include data for one or more connections, simply select additional connections from the "Connection" popup.

Reference Number and Organization

To integrate VPN Tracker's accounting with your own time tracking or billing system, an organization and a reference number can be set for each of your VPN connections in the → Notes tab

Exporting Connections **PRO**

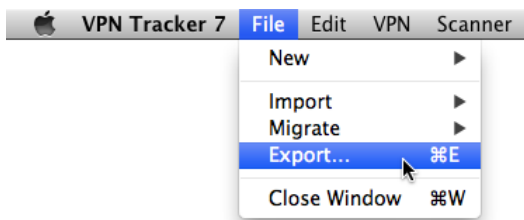
Whether you're quickly exporting a VPN connection for a co-worker, or rolling out VPN Tracker to hundreds of users, VPN Tracker's sophisticated export and convenient installer is there to help.

Exporting a Connection

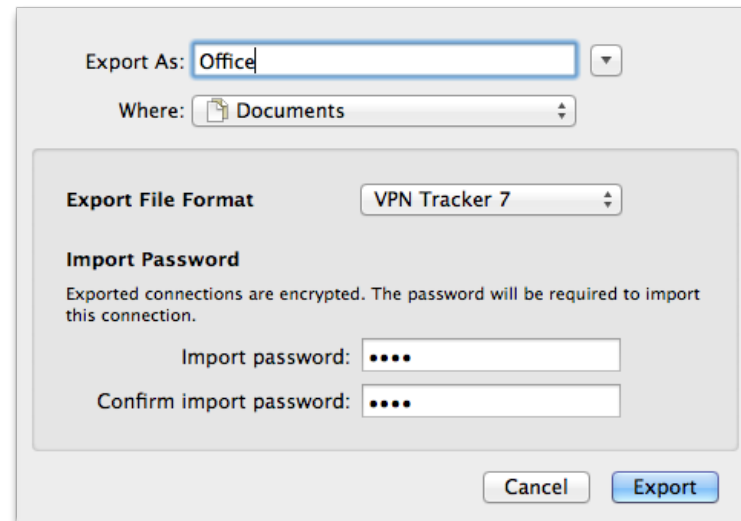
Once you have set up and tested a VPN connection, you can export your connection for other VPN Tracker users.

To export a connection

- ▶ Select the connection
- ▶ Choose „Export...“ from the File menu



- ▶ If you are exporting for users of previous versions of VPN Tracker select the appropriate file format. Not all features are available in previous versions of VPN Tracker. When exporting for earlier versions of VPN Tracker, we recommend testing the exported connection before rolling it out to end users.
- ▶ Set an encryption password for the file. Users of this connection will be required to enter the password once when importing the connection

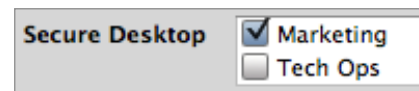


To export multiple connections in a single file, select the connections you would like to export (hold down the ⌘ key to select more than one), and choose File > Export....

Exporting a Secure Desktop

You can also export Secure Desktops for your users, along with their connections. Simply select it along with the connections when exporting (hold down the ⌘ key to select more than one item in the sidebar).

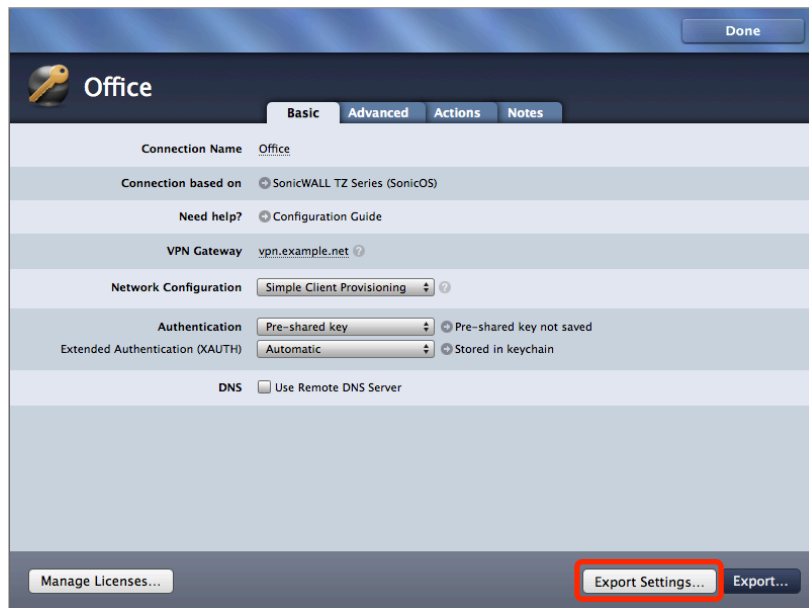
To always export a Secure Desktop with a connection, check the box for this Secure Desktop in the connection's export settings.



Locking Exported Connections

VPN Tracker offers several ways of locking down and protecting your connection information when you export or deploy connections. To change the security settings for an exported connection:

- ▶ Select a connection
- ▶ Click the Configure... button
- ▶ Click „Export Settings...” at the bottom of the window



Now you can password-protect the connection and adjust which information is visible to the user. All security settings are explained in more detail in → *Export Settings Explained*.

Export Settings Explained

Pre-Shared Key	<input checked="" type="checkbox"/> Include pre-shared key from keychain The included pre-shared key will be added to the user's keychain.
	<input checked="" type="checkbox"/> Permit pre-shared keys to be stored in and loaded from the keychain
Extended Authentication (XAUTH)	<input type="checkbox"/> Include XAUTH login and password <input type="text" value="from keychain"/>
	<input checked="" type="checkbox"/> Permit XAUTH credentials to be stored in and loaded from the keychain

Pre-Shared Key

Include pre-shared key from keychain

If you have saved the pre-shared key in your keychain, VPN Tracker can include this pre-shared key with the exported connection.

Permit pre-shared keys to be stored in and loaded from the keychain

Checking this option will (a) move an included pre-shared key into the user's keychain when importing the connection, and (b) permit users to store their pre-shared key in keychain if none is included with the exported connection.



The OS X keychain is a very secure way of storing passwords.

However, users will be able to see the pre-shared key via the Keychain Access application.

If you include a pre-shared key but don't permit storing the pre-shared key in keychain, the pre-shared key will be left in the connection. **This is less secure in terms of encryption, but will prevent a user from seeing the pre-shared key.**

Extended Authentication (XAUTH)

Include XAUTH login and password

If you are using Extended Authentication (XAUTH), you can also include a user's XAUTH credentials (username and password) in the exported connection. Select whether you would like to include the username and password stored in your keychain, or be asked for an XAUTH username and password when exporting the connection.

Permit XAUTH credentials to be stored in and loaded from the keychain

Checking this option will (a) move included XAUTH credentials into the user's keychain when importing the connection, and (b) permit users to store their XAUTH password in keychain if none is included with the exported connection.

Security

Security	<input checked="" type="checkbox"/> Don't allow settings to be changed
	<input type="checkbox"/> Hide settings and detailed logs
	<input checked="" type="checkbox"/> Temporarily permit editing with unlock password
	Unlock password
	Confirm unlock password

Don't allow settings to be changed

This settings prevents users from making accidental or undesirable changes to their VPN connections. The connection is "locked". Users will be able to see the connection settings, but will not be able to modify them.

Hide settings and detailed logs

Hides the Basic and Advanced tabs, as well as the more detailed log levels. Only basic logging and troubleshooting information is displayed. Technical Support Reports cannot be created unless an unlock password is set.

Temporarily permit editing with unlock password

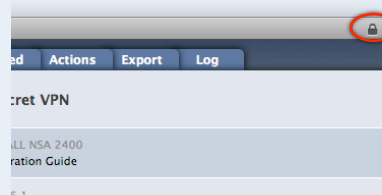
With an unlock password, the connection can be unlocked temporarily, for example if an administrator needs to make changes at a user's computer, or to read the contents of Technical Support Reports.



If you do not set an unlock password, there will be no way to ever make any changes to the exported connection or use a Technical Support Report to analyze a technical problem.

Unlocking a Locked Connection

A locked connection has a padlock icon in the top right corner of the window. Click it to enter the unlock password and access all settings.



Temporarily unlock a locked connection by clicking the padlock in the upper right corner of the window.

Secure Desktop	<input checked="" type="checkbox"/> Marketing Resources
	<input type="checkbox"/> Admin
	<input type="checkbox"/> Accounting
Actions	<input type="checkbox"/> Include actions
Contact Info	helpdesk@example.com
	This email address is the default recipient for Technical Support Reports

Secure Desktop

If you have configured a Secure Desktop, you can choose to include it with your exported connection.

Use a Secure Desktop to provide your users with a familiar environment for everything they need to do over VPN – network shares, websites, databases, and applications.

Secure Desktops selected here are always included when exporting this connection. If you'd like to export additional Secure Desktops, simply select them together with your connection before exporting.



You can configure → *Direct Link Detection* so your users are able to use Secure Desktop even when no VPN is required, e.g. when connected directly to the office network.

Actions

If you have configured actions to be executed when the connection is connected or disconnected, you can include them as well. Any settings you have configured in your connection's "Actions" tab will be included.

Contact info

If your VPN users run into any issues, they can email you a Technical Support Report with details about their connection settings, local internet connection and VPN logs. The email address you enter as your contact info will be set as the default recipient of the report.

Other Day-to-Day Considerations

Unlock Password

Experience has shown that when exporting a locked connection, you'll want to unlock it at one point or the other – whether it's making a quick change at an end user's Mac, accessing an end user's Technical Support Report, or even importing the (locked) connection onto your own Mac and accidentally replacing the (unlocked) original.

- ▶ If you do not set an unlock password for a locked connection, there is no way to ever change settings.
- ▶ If you do not set an unlock password and hide the settings and logs, there's no way to ever access the setting.

We therefore strongly recommend always setting an unlock password.

Certificates

If your connection uses certificates for authentication, keep in mind that the certificates are not included with the exported connection. You'll need to distribute the certificates as you would normally do.

VPN Tracker will automatically attempt to use the same certificates on the Mac where the connection is imported. If they are not available, the user will be prompted to select new certificates. For additional information, please refer to → *Certificates*.

Overwriting Existing Connections

If you have made changes to an connection that you already distributed to your users earlier, it's a good idea to re-use the same connection when exporting (don't create a new one).

That way your users will be prompted to replace their existing connection with the updated one, instead of ending up with another copy, and in the end not knowing which connection is the current one.



VPN Tracker Deployment Guide

- ▶ Are you deploying VPN Tracker to end users in your organization?
- ▶ Are you a consultant setting up VPN Tracker for your clients?
- ▶ Are you managing the VPN Tracker licenses in your organization?

Get the VPN Tracker Deployment Guide for up-to date information and best practices. Download your free copy today at <http://www.vpntracker.com>

Troubleshooting

In most cases, your connection will work fine if you follow the instructions in this manual. However, computer networking and VPN are complex, so sometimes problems do occur. Read this chapter to learn how to resolve them.

Missing Settings

If you forgot to fill in a setting, VPN Tracker will point it out to you:



Simply fill in the missing information, then try connecting again.

Connection Errors

In case of any other problem, a yellow warning triangle will show up:



Click the yellow warning triangle to be taken to the log. The log will explain exactly what the problem is. Follow the steps listed in the log to resolve the problem.



Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem.

If you need additional help, you can email the log to your administrator, or send a Technical Support Report to equinux or to your administrator.



A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is **not** included in a Technical Support Report. If you contact equinux technical support, always include a Technical Support Report.

No Access to the Remote Network

If you find yourself in a situation where your VPN appears to be connected, but you cannot access resources (servers, email, etc.) in the remote network, check the following points to resolve the problem.



Connect to an IP address (instead of a host name)

If you are using a host name (e.g. fileserver.example.com) to connect to the resource, please try using its IP address instead.

If the connection works when using the IP address, but not when using a host name, please make sure that your Mac's DNS server is able to resolve this host name to an IP address, or set up a suitable remote DNS server in VPN Tracker. See → *Troubleshooting Remote DNS* for more information.

Browsing the Network – Bonjour and VPN

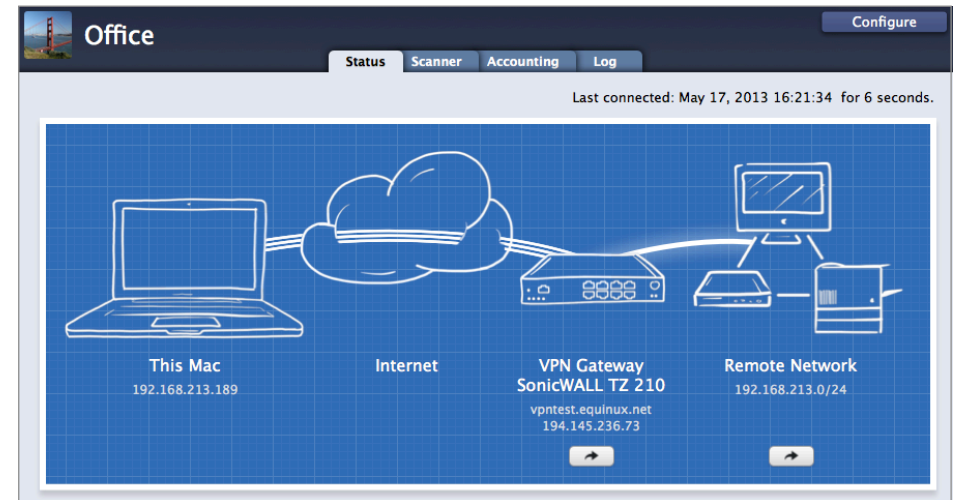
Bonjour is the technology that makes your file servers appear in your Finder's sidebar. It depends on broadcasts on the local network. These broadcasts do not travel over VPN. If you are connecting to servers over VPN, you will therefore need to use their IP address (or DNS host name, if using remote DNS).

To learn more about how to connect to servers over VPN, see → *Secure Desktop* and → *Accessing Files, Printers and Databases*

Check that the IP address you are connecting to is part of the VPN's remote network

Check that the IP address you are connecting to is part of the remote network(s) of the VPN. Also double-check the network mask that you have configured for the remote network(s) in VPN Tracker.

If you are using SonicWALL Simple Client Provisioning or Cisco EasyVPN, the remote network(s) are assigned by your VPN gateway. You can see the remote network(s) on the Status tab.



About Subnet Masks and Routing Prefixes

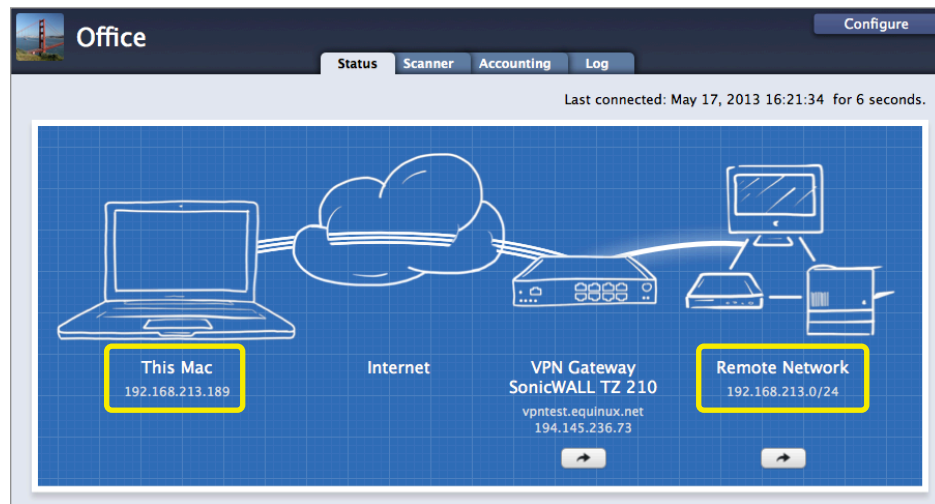
A network mask determines the size of the network. For IPv4 networks, it can be written in two ways: As a subnet mask (e.g. 255.255.255.0) or as a routing prefix (e.g. /24). For IPv4 it does not make a difference which one is used. If you enter a subnet mask, VPN Tracker will automatically convert it to a routing prefix (CIDR notation).

Lets take a look at the network 192.168.42.0 / 255.255.255.0 (which is the same as 192.168.42.0/24). This network contains all IP addresses that begin with 192.168.42., for example 192.168.42.1 and 192.168.42.99. It does not contain 192.168.43.1 or 10.1.2.3.

Make sure the host you are trying to reach knows where to send replies

This one is a little more complex to check. Start with checking if your local address is part of the remote network:

- ▶ Connect the VPN
- ▶ Go to the Status tab
- ▶ Compare the IP address listed under “This Mac” (local address) and the networks listed under “Remote Network”. Is the local address part of the remote network(s)?



In this example, the local address 192.168.213.189 is part of the remote network 192.168.213.0/24

If the local address is part of the remote network(s):

There are exactly three setups where the local IP address may be part of the remote network(s). If your setup is not one of these, you must choose a local address that is **not** part of the remote network(s).

1. When connecting to a SonicWALL using SonicWALL Simple Client Provisioning or DHCP over VPN.
2. When connecting to a Cisco VPN gateway using Cisco EasyVPN.

3. When connecting to a VPN gateway that can act as an ARP proxy for IP addresses assigned through Mode Config, and/or for fixed local addresses.

That third one is a bit tricky to figure out. If you find a reference to ARP Proxy (or Proxy ARP) in the device's documentation, or if the manual specifically instructs to choose the local address or the Mode Config address pool to be part of the remote network, then it's ok for the IP address to be part of the remote network.

In all other cases you must choose an IP address as the local address (or a Mode Config address pool) that is not part of the remote network(s). If you are using Mode Config, you need to change the Mode Config address pool on the VPN gateway. Otherwise, simply change the local address in VPN Tracker (Basic > Local Address).

If the local IP is not part of the remote network(s):

Check if your VPN gateway is the default gateway (router) of its network.

If your VPN gateway is not the default gateway of the remote network, you will have to ensure that responses to all IP addresses used by VPN clients are routed to the VPN gateway. You can do so either by adding a general route on the network's actual default gateway, or by adding individual routes on each host that VPN clients need to communicate with.

Troubleshooting Remote DNS

If you can access resources on the remote network using their IP addresses, but not their host names, you will need a suitable remote DNS setup.

Prerequisites for remote DNS:

- ▶ A DNS server that is able to resolve those IP addresses exists.
- ▶ The DNS server can be reached through the VPN.

To illustrate the steps for debugging remote DNS issues, here's an example setup using remote DNS:

- ▶ We have a VPN connection to the remote network 192.168.42.0/24.
- ▶ In this network, there's a file server *fileserver.example.com*.
- ▶ We can reach this file server using its IP address 192.168.42.10.
- ▶ We'd like to reach this file server using its host name *fileserver.example.com*.
- ▶ This host name cannot be looked up using public DNS servers, but there is an internal DNS server with IP address 192.168.42.2 that is able to resolve hosts in the *example.com* domain, including *fileserver.example.com*.



For remote DNS settings to take effect, the VPN needs to be reconnected. We should now be able to connect to *fileserver.example.com* using its host name.

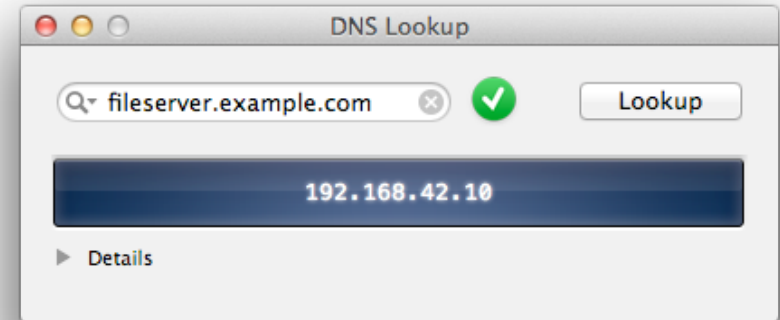


If you set a remote DNS server for "All Domains" instead of specific "Search Domains", make sure it is a working DNS server that can resolve hosts on the Internet. Otherwise, your Mac will seem to be cut off from the Internet when the VPN is connected.

Steps to Troubleshoot

If connecting using the host name does not work, the first step is to use the DNS Lookup Tool to verify that the host name can be looked up.

- ▶ Connect the VPN
- ▶ Choose Tools > DNS Lookup from the menu bar on top of the screen
- ▶ Enter the host name (here: *fileserver.example.com*) and click "Lookup"



If the DNS Lookup Tool displays the expected result, remote DNS is configured correctly. In that case, the problem is with the actual connectivity, not DNS.

If DNS lookup fails, then the problem is with remote DNS. The next step is to figure out if the problem is with the remote DNS server itself, or with the remote DNS setup.

- ▶ Open a Terminal window (Applications > Utilities > Terminal)
- ▶ Enter: `dig <host name> @<remote DNS server>` and press return. In our example: `dig fileserver.example.com @192.168.42.2`

If you see an "Answer Section" with the correct IP address, then both the connectivity to the DNS server, and the DNS server's response are ok. In that case, the problem lies with the remote DNS setup. Double-check the configuration in VPN Tracker.

```
# dig fileserver.example.com @192.168.42.2
; <<> DiG 9.7.6-P1 <<> fileserver.example.com @192.168.42.2
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 30106
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
fileserver.example.com.      IN A

;; ANSWER SECTION:
fileserver.example.com.     3600    IN A    192.168.42.10

;; Query time: 879 msec
```

If you don't see an "Answer Section" with the correct IP address, then the remote DNS server is not configured to resolve *fileserver.example.com*.

If you get a timeout error, then the remote DNS server is not reachable over the VPN or it is not a properly configured DNS server.



Some DNS servers are configured to talk only to specific hosts or networks. When connected through the VPN, your Mac may not be part of these. Check your DNS server's settings or ask the DNS server's administrator to be sure.

DNS Troubleshooting Advice for Experts

Command-line tools like `nslookup` and `dig` do **not** accurately reflect DNS resolution on modern OS X versions (but can be very helpful in debugging connections to and results from a single DNS server, as we did above).

- ▶ To get exactly the DNS results an OS X application would receive, use the DNS Lookup Tool in VPN Tracker (Tools > DNS Lookup)
- ▶ The DNS settings (and search domains) assigned by the VPN gateway using Mode Config, Cisco EasyVPN, or SonicWALL Simple Client Provisioning / DHCP over VPN, are displayed in the connection log and in the "Network" section of the → *VPN Connection Stats*.
- ▶ To see the Mac's currently applicable DNS settings, including those set by VPN Tracker for remote DNS use the Terminal command `scutil --dns`.

Further Questions?

You can find the latest news and compatibility information on our support and FAQ website:

<http://equinux.com/support>

Contacting Technical Support

If you can't resolve your issue with the information available on our website or in this guide and would like to contact Technical Support through our website, please be sure to include the following information:

- ▶ The manufacturer and model and firmware revision of the VPN gateway
- ▶ A Technical Support Report from VPN Tracker (Help > Generate Technical Support Report)
- ▶ Screenshots of what you have configured on your VPN gateway, in particular all VPN-related settings
- ▶ A detailed description of the problem and the troubleshooting steps you have already taken

Reference

Settings Reference

This chapter describes the settings available in VPN Tracker. Settings are grouped by location and sorted from top to bottom as they occur in VPN Tracker. Where possible, related settings and the corresponding settings on a VPN gateway (and the terms different vendors use) are also included.

Basic Tab

The screenshot shows the 'Basic' tab of the VPN Tracker settings interface. At the top, there are tabs for 'Basic', 'Advanced', 'Actions', 'Export', and 'Log'. Below the tabs, there is a section titled 'My connection' with a dashed box icon. The settings are organized into several sections: 'Connection based on' with options for 'Custom Device' and 'Configuration Guide'; 'VPN Gateway' with a text input field for 'Hostname or IP Address'; 'Network Configuration' with dropdown menus for 'Manual Configuration', 'Topology' (set to 'Host to Network'), 'Local Address' (set to 'IP Address'), and 'Remote Networks' (set to 'Network Address'); 'Authentication' with a dropdown for 'Pre-shared key' (with a note 'Pre-shared key not saved') and 'Extended Authentication (XAUTH)' set to 'Off'; 'Identifiers' with dropdowns for 'Local' and 'Remote' (both set to 'Fully Qualified Domain Name (FQDN)') and corresponding text input fields for 'Local Identifier' and 'Remote Identifier'; and 'DNS' with a checkbox for 'Use Remote DNS Server'.

Connection Name

A name for the connection. You may choose any name you like.

Availability: always (use the Edit menu to change the name if locked)

VPN Gateway

The public IP address or host name of the VPN gateway to connect to.

Related Settings: Advanced > IPv6 > Use IPv6 VPN gateway address when available

Availability: always

VPN Gateway Setting: WAN IP address, public IP address, external IP address

Network Configuration

VPN Tracker supports a number of vendor-specific and vendor-independent automatic configuration methods.

Mode Config

A vendor-independent automatic configuration method that is capable of transmitting the settings for the local address and the remote DNS settings (DNS servers and search domain).

The "active" and "passive" variants are used to resolve interoperability issues with some devices.

Related Settings: Basic > Network Configuration > Local Address
Basic > Remote DNS > Receive DNS Settings from VPN Gateway

Availability: Depending on the selected device profile. Use a custom device profile to be able to select any method.

VPN Gateway Setting: Mode Config, Config Mode, IKE-CFG

Cisco EasyVPN

An extension of Mode Config for Cisco devices that is also capable of transmitting the Remote Network(s) and Perfect Forward Secrecy (PFS) setting.

The "passive" variant can be used to resolve problems when the general EasyVPN setting does not work with a particular device.

If you are using EasyVPN with a custom device profile, make sure to turn on "Identify as Cisco Unity Client" on the Advanced tab.

Related Settings: Basic > Network Configuration > Local Address
Basic > Network Configuration > Remote Networks
Basic > Remote DNS > Receive DNS Settings from VPN Gateway
Advanced > Interoperability > Cisco

Availability: Depending on the selected device profile. Use a custom device profile to be able to select any method.

VPN Gateway Setting: No special settings are needed to use Cisco EasyVPN with EasyVPN-capable Cisco devices. For more details, refer to our Cisco configuration guides.

SonicWALL DHCP over VPN

An automatic configuration method implemented by SonicWALL devices that is capable of transmitting the settings for the Local Address and the Remote DNS settings (DNS servers and search domain).

Related Settings: Basic > Network Configuration > Local Address
Basic > Remote DNS > Receive DNS Settings from VPN Gateway

Availability: Depending on the selected device profile. Use a custom device profile to be able to select any method.

VPN Gateway Setting: GroupVPN > Client > Virtual Adapter Setting > DHCP Lease (or DHCP Lease or Manual Configuration) + suitable configuration for DHCP server and VPN > DHCP over VPN.

SonicWALL Simple Client Provisioning (SCP)

An automatic configuration method implemented by SonicWALL devices that can supply all settings of a VPN connection to the client.

Related Settings: Basic > Remote DNS > Receive DNS Settings from VPN Gateway

Availability: Depending on the selected device profile. Use a custom device profile to be able to select any method.

VPN Gateway Setting: No special configuration needed. Requires SonicOS 4.0 or newer.

Topology

In most cases, the topology should be set to **Host to Network**. This means that a single host (= your Mac) connects to one or more remote networks through VPN. Only network traffic destined for these networks is sent through the VPN, all other traffic is sent out unmodified through the Mac's Internet connection.

Other possible topologies are:

Host to Everywhere

A single host tunneling all its Internet traffic through VPN. This is equivalent to a Host to Network connection with a remote network of 0.0.0.0/0.

For Host to Everywhere to work, the VPN gateway must accept a policy with a 0.0.0.0/0 endpoint, and also take care of the routing and Network Address Translation (NAT) for the VPN client when it tries to access the Internet.

Network to Network **PRO**

A (local) network being connected to another (remote) network, with the Mac running VPN Tracker acting as the local VPN gateway, and another VPN gateway at the remote end. This can be used to connect a branch or home office with multiple computers to a main office. The Mac running VPN Tracker needs to have routing enabled and has to be configured as the router for the other computers that are to use the VPN.

Host to Host

A single host (= your Mac) accessing another single host (e.g. a single file server, email server etc.) through VPN.

Related Settings: Basic > Local Address, Basic > Network Configuration, Basic > Remote Networks

Availability: Not available with Cisco EasyVPN and SonicWALL Simple Client Provisioning. Network to Network requires VPN Tracker Pro.

VPN Gateway Setting: Set default route as this gateway (SonicWALL), Allow all traffic through tunnel (WatchGuard), or determined implicitly by VPN endpoints.

Local Address

The local address is the IP address that the Mac running VPN Tracker uses in the remote network when connected through VPN¹.

If the local address is left empty, the current IP address of the Mac's en0 network interface will be used. Since this is most likely a private IP address, it is not unique worldwide. In order to avoid situations where two clients coming in through VPN using the same IP, **do not leave the local address empty when you have multiple VPN users**. In that case, always set a unique local address for each client.

The local address should be from a *private subnet*, and must **not** be part of the remote network(s) of the VPN connection (unless the documentation of your VPN gateway specifically instructs you to do so²).

Related Settings: Basic > Topology, Basic > Network Configuration

Availability: Not available when an automatic configuration method is being used. When a Network to Network topology is used, the setting is called "Local Networks" and describes the local network(s) to which the VPN tunnel applies.

VPN Gateway Setting: Remote (IP) address, peer (IP) address, remote endpoint, remote network

¹ In IPsec terms: the local endpoint of the IPsec Security Association (SA)

² Such VPN gateways typically have you configure a specific IP address for the client to use and/or have a setting called "Proxy ARP" or "Tie remote stations into the LAN"

³ In IPsec terms: the remote endpoint of the IPsec Security Association (SA)

Remote Networks

The network(s) the VPN connects to³. Traffic destined for these network(s) will be tunneled over the VPN.

The network(s) can be entered in CIDR notation (e.g. 192.168.42.0/24) or – for IPv4 connections – using the subnet mask (e.g. 192.168.42.0/255.255.255.0).

Always make sure you are using a correct network address. VPN Tracker will try to help you with this, so it might change your input to turn it into a correct network address. Please double check the changes that VPN Tracker made, and correct them if necessary.

Related Settings: Advanced > Phase 2 > Establish a separate tunnel for each remote network, (Cisco only) Advanced > Interoperability > Cisco > Establish a shared tunnel to 0.0.0.0/0 for split-tunneling

Availability: Not available when EasyVPN or SonicWALL Simple Client Provisioning are used. For these setups, the VPN gateway supplies the networks.

When a Host to Host topology is used, the setting is called "Remote Address" and describes the single remote address the VPN tunnel applies to.

VPN Gateway Setting: Local (IP) address, local endpoint, local network

Authentication

The authentication method VPN Tracker uses. Three methods are available:

Pre-Shared Key

The VPN client is authenticated using a shared password, the pre-shared key. This is the most commonly used authentication method.

It is possible to store the pre-shared key in the OS X keychain, or be prompted every time the VPN connections.

Certificate

The VPN client and the VPN gateway mutually authenticate using X.509 certificates (RSA signatures). This method is very secure, but requires an infrastructure for creating and distributing certificates, and a VPN gateway that supports it.

The client's certificate and private key (also called an "identity") need to be present in the OS X keychain.

The VPN gateway's certificate can in most cases be sent by the VPN gateway and verified just as a web browser would do for HTTPS, however, it is also possible to add it to the local keychain and select that specific certificate in VPN Tracker.

Hybrid Mode

The VPN gateway authenticates itself with a certificate, and users authenticate themselves through Extended Authentication (XAUTH). This method is supported by a small number of vendors (e.g. Check Point) and considered more secure than using an Aggressive Mode connection with just a pre-shared key.

The VPN gateway's certificate can in most cases be sent by the VPN gateway, but it is also possible to add it to the local keychain and set that specific certificate in VPN Tracker.

Related Settings: (certificates only) Advanced > Certificates (pre-shared key only) Advanced > Phase 1 Diffie-Hellman Group, Advanced > Additional Settings > Credentials

Availability: According to the selected device profile.

VPN Gateway Setting: (Pre-Shared Key) Pre-shared secret, shared secret, password, key, (Certificates) X.509 certificates, RSA signatures

Extended Authentication (XAUTH)

Extended authentication is a way of authenticating individual users on top of one of the general authentication methods, pre-shared key or certificates (hybrid mode already incorporates XAUTH).

In its basic form, XAUTH asks for a username and password, however it is also possible for the VPN gateway to ask for passcodes (such as the ones generated by RSA SecurID tokens) etc.

It is possible to store the XAUTH username and password in the OS X keychain, or be prompted every time the VPN connections.



XAUTH can be set to "Automatic", even if it is actually turned off on the VPN gateway. The VPN gateway will tell VPN Tracker if XAUTH should be used or not. However, there are VPN gateways that need XAUTH specifically turned on or off, that's where the "Off" and "Always" settings can help.

Related Settings: Advanced > Additional Settings > Credentials

Availability: According to the selected device profile.

VPN Gateway Setting: XAUTH, user authentication

Identifiers

The identifiers are small pieces of identifying information that VPN Tracker and the VPN gateway use to recognize each other.

Related Settings: Basic > VPN Gateway (for "Remote Endpoint IP Address") Basic > Authentication > Certificates (for "Local/Remote Certificate")

Availability: Identifiers are determined automatically if SonicWALL Simple Client Provisioning is used.

VPN Gateway Setting: The local identifier from VPN Tracker's perspective is the remote (!) identifier from the VPN gateway's perspective, and vice versa. Therefore you will normally have to swap the identifiers configured on the VPN gateway when entering them in VPN Tracker:

Local Identifier: Remote Identifier (or client/peer identifier/identity/ID)
Remote Identifier: Local Identifier (or own/my identifier/identity/ID)

Local Identifier

The identifier that VPN Tracker uses to identify itself to the VPN gateway. The VPN gateway uses the identifier to map the incoming connections to the VPNs it has configured.



Make sure that the local identifier type and value in VPN Tracker match what the VPN gateway expects! Otherwise the VPN gateway may refuse or silently drop the connection.

IP Address

An IP address is used for identification. Make sure to enter the IP address the VPN gateway expects.

Local Endpoint IP Address

Same as “IP Address,” but VPN Tracker will automatically use the Mac’s current local IP address as the value. Useful if your VPN gateway permits incoming connections using any IP address-based identifier.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name (FQDN) is used for identification (e.g. client.example.com).

Email (User FQDN)

An email address is used for identification (e.g. vpntracker@example.com).



Some VPN gateways expect FQDN or User FQDN type identifiers that are neither valid FQDNs nor email addresses. This is ok. Simply enter whatever your VPN gateway expects you to use (e.g. a connection identifier, user name or group name).

Key ID

An identifier for vendor-specific use. Cisco EasyVPN devices use this for the group name of the connecting user.

ASN.1 DN

An ASN.1 Distinguished Name (DN) is used for identification. Normally this is used in conjunction with certificate-based authentication. Enter the (correctly formatted) ASN.1 DN that the VPN gateway expects.

Local Certificate

The identifier is the ASN.1 Distinguished Name taken from the subject of the local certificate (only possible when using certificates for authentication).

Remote Identifier

The identifier that VPN Tracker should expect from the VPN gateway. VPN Tracker will compare the actual identifier sent by the VPN gateway to the one configured here. If the identifiers do not match, the connection attempt will be stopped and an error displayed in the log.

Don’t verify remote identifier

Turn off identifier verification (e.g. for testing). Identifier verification provides minor security benefits for Aggressive Mode connections, but should always be used for Main Mode connections.

IP Address

An IP address is used for identification. Enter the IP address the VPN gateway sends. It is often, but not always, the VPN gateway’s public IP address.

Remote Endpoint IP Address

Same as “IP Address,” but VPN Tracker will automatically use the public IP address of the VPN gateway.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name (FQDN) is used for identification (e.g. vpn.example.com). Enter the FQDN the VPN gateway sends.

Email (User FQDN)

An email address is used for identification (e.g. vpnservice@example.com). Enter the email address the VPN gateway sends.



Some VPN gateways use FQDN or User FQDN type identifiers that are neither valid FQDNs nor email addresses. This is ok. Simply enter whatever your VPN gateway sends as its identifier.

Key ID

An identifier for vendor-specific use.

ASN.1 DN

An ASN.1 Distinguished Name (DN) is used for identification. Normally used in conjunction with certificate-based authentication. Enter the (correctly formatted) ASN.1 DN that the VPN gateway sends.

Remote Certificate

The identifier is the ASN.1 Distinguished Name taken from the subject of the remote certificate (only possible when using certificates for authentication).

DNS

Use Remote DNS Server

VPN Tracker can use a name (DNS) server in the remote network of the VPN to look up certain (or all) host names. This is useful if your organization operates an internal DNS server that can look up host names of computers on the internal network.

Availability: always

Receive DNS Settings from VPN Gateway

When checked, VPN Tracker will use the DNS settings transmitted by the VPN gateway during automatic configuration. To see if your VPN gateway transmits such information, turn off Remote DNS, then connect. VPN Tracker will show a message in the log suggesting to turn on Remote DNS if settings have been transmitted.

Related Settings: Basic > Network > Automatic Configuration
Basic > DNS > Use Remote DNS Server

Availability: Available if an automatic configuration method is selected and “Use Remote DNS Server” is turned on.

DNS Servers

The IP address of a remote DNS server. To enter more than one server, click the plus button to get additional input fields.

Related Settings: Basic > DNS > Use Remote DNS Server
Basic > DNS > Use DNS Server for

Availability: Available if “Use Remote DNS Server” is turned on, and “Receive DNS Settings from VPN Gateway” is turned off.

Search Domains

The search domain(s) to use. To enter more than one search domain, click the plus button to get additional input fields.

If “Use DNS Server for” is set to “Search Domains”, the search domain(s) will also be used to determine the domains the remote DNS server is being used for.

Related Settings: Basic > DNS > Use Remote DNS Server
Basic > DNS > Use DNS Server for

Availability: Available if “Use Remote DNS Server” is turned on, and “Receive DNS Settings from VPN Gateway” is turned off.

Use DNS Server for

This setting determines the scope of the remote DNS server(s). It is possible to use the remote DNS server(s) for all DNS lookups, or just for hosts in a specific domain.

All Domains

While the VPN is connected, the remote DNS server is used for every DNS lookup on this Mac, not just hosts that are part of the remote network.



When using this option, it is important to make sure the VPN connection and the remote DNS server are correctly configured: If one or both are not working, the Mac will appear to be cut off from the Internet while the VPN is active.

Search Domains

The remote DNS server is used only for looking up host names that are part of the search domain(s). At least one search domain must be configured.

Search Domains (if available)

“Receive DNS Settings from VPN gateway” only: If the VPN gateway transmits a search domain, the remote DNS server is used only for looking up host names that are part of the search domain(s). If no search domain is transmitted, the remote DNS server is used for every DNS lookup on this Mac while the VPN is connected.

Related Settings: Basic > DNS > Search Domains
Basic > DNS > Use Receive DNS Settings from VPN Gateway

Availability: Available if “Use Remote DNS Server” is turned on.

Use for reverse lookup of IP addresses in remote networks

The remote DNS server is used for reverse lookups (mapping IP addresses back to host names) in the remote networks. When the remote DNS server is used for “All Domains”, this happens automatically.

Related Settings: Basic > Network Configuration > Remote Networks
Basic > DNS > Use DNS Server for

Availability: Available if “Use Remote DNS Server” is turned on.



Need more help configuring your remote DNS setup? A chapter on → *Troubleshooting Remote DNS* is available in this manual.

Advanced Tab

The screenshot shows the 'Advanced' tab of a VPN configuration interface. It is divided into several sections:

- Phase 1:**
 - Exchange mode: Aggressive Mode
 - Lifetime: 28800 seconds
 - Encryption algorithm: AES-128, 3DES (checked)
 - Hash algorithm: SHA1, MD5 (checked)
 - Diffie-Hellman: Group 2 (1024 bit)
- Phase 2:**
 - Lifetime: 28800 seconds
 - Encryption algorithm: AES-128, 3DES (checked)
 - Authentication algorithm: HMAC SHA1, HMAC MD5 (checked)
 - Perfect Forward Secrecy (PFS): DH Group 2 (1024 bit)
 - Establish a separate phase 2 tunnel for each remote network
- NAT-Traversal:** Automatic
- Connection timeout:** 30 seconds (retry every 5 seconds, up to 5 times)
- Interoperability:**
 - General:**
 - Send INITIAL-CONTACT message
 - Important: If you select this option, some devices may disconnect other VPN users.
 - Advertise as Dead Peer Detection (DPD) capable
 - Perform active Dead Peer Detection every 20 seconds if necessary
 - Use VPN Tracker 6 as the application version during Mode Config
 - Cisco:**
 - Send Cisco Unity Vendor ID
 - Send Cisco firewall attribute during Mode Config
 - Establish a shared tunnel to 0.0.0.0/0 for split-tunneling
- IPv6:** Prefer IPv6 VPN gateway address, if available

Establishing the VPN: Phases, Proposals and Device Profiles

An IPsec VPN connection is established in two phases. In phase 1, VPN Tracker and the VPN gateway verify each other's identity and negotiate encryption keys through which the actual setup of the VPN, phase 2, will be secured.

- ▶ In each phase, VPN Tracker sends the algorithms it is willing to use, as well as a few other settings to the VPN gateway (the "proposals"). The algorithms that VPN Tracker sends are determined by the settings for Phase 1 and 2 on the Advanced tab.
- ▶ The VPN gateway then selects one set of algorithms, or responds with an error (typically something like "no proposal chosen") if it does not agree to use any of the proposed algorithms.

At first glance, it would seem a good idea to simply propose all possible algorithms to the VPN gateway, hoping that it will agree with at least one proposal. However, there are several problems with this approach:

- ▶ Selecting too many algorithms causes data packets on the network to be so large they need to be split up ("fragmented"). Many VPN gateways outright refuse these fragmented VPN packets, and intermediate routers often have difficulties with fragmented VPN data packets as well.
- ▶ Some VPN gateways refuse connection attempts altogether that contain many proposals or algorithms unsupported by the VPN gateway, most likely to serve as an intrusion prevention measure.
- ▶ It is desirable to offer only those algorithms providing a very high level of security.

In the device profiles shipping with VPN Tracker, two or three algorithms that are most commonly used with a given device have been selected.

This increases the chance of a successful connection, even if the exact configuration is not known (while still keeping the data packets small enough to not be fragmented). However, if you know your VPN gateway's exact configuration, it is best to select exactly one proposal (combination of encryption, authentication/hash algorithm, and DH group) that your VPN gateway is set up to use.

Phase 1

In phase 1, using the pre-shared key or RSA signatures, VPN Tracker and the VPN gateway negotiate encryption keys with which the set up of the actual VPN tunnel (phase 2) will be secured, and verify each other's identity.

Related Settings: Basic > VPN Gateway, Basic > Network Configuration > Automatic Configuration, Basic > Authentication, Basic > Identifiers

Availability: Phase 1 settings are not configurable when SonicWALL Simple Client Provisioning is used.

VPN Gateway Setting: Phase 1 proposals, phase 1, IKE

Exchange Mode

The Exchange Mode determines how the initial steps of establishing a VPN connection take place. The setting must match the exchange mode selected on the VPN gateway.

Aggressive Mode

Aggressive Mode is faster and requires less information, in particular, it does not require the IP address of the connecting client to be known prior to connecting.

Main Mode

Main Mode is more secure but often requires the IP address of the connecting client to be known beforehand.



Most VPN gateways only support Aggressive Mode connections for VPN clients connecting from dynamic IP addresses or from behind a NAT router.

Lifetime

For security reasons, the encryption keys of a VPN connection are periodically re-negotiated. The lifetime determines when this takes place. The setting must match the lifetime for phase 1 on the VPN gateway, however a misconfiguration will usually not show up right away, but will only be recognizable when the re-negotiation does not work properly.



If you are setting up your VPN gateway from scratch: It is common to select a lifetime of between 1 and 24 hours (3600 to 86400 seconds).

Encryption Algorithm

The encryption algorithm to use for phase 1 of the connection. It must match the algorithm configured on the VPN gateway for phase 1.



If you are setting up your VPN gateway from scratch: Each VPN gateway uses different hardware and has a different selection of algorithms available, however, most support at least one of AES-128, 3DES or DES, so if there is no information what your VPN gateway might be using, try those.

AES-256 is considered to be the most secure algorithm. All AES variants and 3DES provide reasonably good security. Use DES only if there's no better choice.



In case you do not know what is configured on your VPN gateway, it is possible to select more than a single algorithm. VPN Tracker will then offer all selected algorithms to the VPN gateway and negotiate which one to use.

To avoid fragmentation of network packets or triggering intrusion prevention mechanisms on VPN gateways, it is not recommended to select more than two or three algorithms

Hash Algorithm

The hash algorithm used for phase 1 of the connection. It must match the algorithm configured on the VPN gateway for phase 1.



If you are setting up your VPN gateway from scratch: Use SHA-1 if possible. Only use MD5 if no other algorithm is available.

If you own a modern device, it is possible that it already supports SHA-2, which offers additional security.



In case you do not know what is configured on your VPN gateway, it is possible to select both SHA-1 and MD5 here, most VPN gateways will be able to negotiate which one they want to use.

Diffie-Hellman (DH) Key Exchange

The key length to use for the Diffie-Hellman key exchange. It must match the key length (group) selected on the VPN gateway for phase 1.

If you are getting inexplicable errors about an incorrect pre-shared key, double-check that the Diffie-Hellman group matches the VPN gateway's configuration.



If you are setting up your VPN gateway from scratch: Choose at least "Group 2 (1024 bit)" whenever possible.

Many VPN gateways support up to "Group 5 (1536 bit)", and it is a good idea to use that if it is available. Some recent high-end devices support up to "Group 18 (8192 bit)".

Phase 2

This second phase of the connection establishes the actual VPN tunnel. All settings here must match the respective setting on the VPN gateway.

Related Settings: Basic > Network Configuration

Availability: Phase 2 settings are not configurable when SonicWALL Simple Client Provisioning is used.

VPN Gateway Setting: Phase 2 proposals, phase 2, IPsec, VPN, tunnel

Lifetime

For security reasons, the encryption keys of a VPN connection are periodically re-negotiated. The lifetime determines when this takes place. The setting must match the lifetime for phase 2 on the VPN gateway, however a misconfiguration will usually not show up right away, but will only be recognizable when the re-negotiation does not work properly.



If you are setting up your VPN gateway from scratch: The lifetime for phase 2 can be different from the phase 1 lifetime, if it is, it is typically shorter. It is common to select a lifetime of between 1 and 24 hours (3600 to 86400 seconds).

Encryption Algorithm

This is the algorithm used for encrypting the actual data that goes over the connection. See Advanced > Phase 1 > Encryption Algorithm for more information.



If you are setting up your VPN gateway from scratch: The encryption algorithm for phase 2 can be different from the phase 1 encryption algorithm. For VPN gateways with severely limited encryption hardware, it may be appropriate to choose a less secure but better performing algorithm here, and set a more secure algorithm for phase 1.

Authentication Algorithm

See Advanced > Phase 1 > Hash Algorithm.



Do not select "No authentication", unless you have a very special setup that does not support using authentication. **No authentication means exactly what it says and is extremely insecure.**

Perfect Forward Secrecy (PFS)

Using Perfect Forward Secrecy provides additional security when encryption keys are re-negotiated. The setting must match what is configured on your VPN gateway.



If you are setting up your VPN gateway from scratch: Using Perfect Forward Secrecy is recommended.

If you are using a Cisco device with Easy VPN: Cisco devices can transmit their Perfect Forward Secrecy preference. Since using PFS is always more secure, VPN Tracker will use it when requested by a Cisco VPN gateway.

VPN Gateway Setting: Some devices do not have a dedicated setting for the PFS DH group. These devices typically use the same group as for phase 1.

Establish a separate phase 2 tunnel for each remote network

When connecting to multiple remote networks, VPN Tracker can either establish a separate VPN tunnel (Security Association, SA) for each network, or send all traffic over a single tunnel. The single tunnel will use the first remote network as the endpoint.

Which setting to use depends on the VPN gateway. If you find that with a single tunnel you cannot access any remote network but the first, then try swapping the order of the remote networks. If you can now access the new first network, then you likely need this setting turned on (or, less likely, your VPN gateway supports only a single remote network for the connection).

Cisco EasyVPN-based VPN gateways are a special case, here you should almost always uncheck this setting **and** enable "Establish a Shared Tunnel to 0.0.0.0/0 for Split-Tunneling" in the Interoperability settings.

Related Settings: Basic > Network > Remote Networks
Advanced > Interoperability > Cisco > Establish a Shared Tunnel to 0.0.0.0/0 for Split-Tunneling

Availability: The setting is available only if there are multiple remote networks, or when using an automatic configuration method that could lead to connecting to multiple remote networks.

Certificates

Send Certificate

If turned on, VPN Tracker will send the local certificate to the VPN gateway. This setting should normally be turned on. Only turn off this setting if your VPN gateway has trouble dealing with certificates sent by connecting clients.

Related Settings: Basic > Authentication > Certificate

Availability: The setting is only available for certificate-based authentication.

Send Request for Remote Certificate

If turned on, VPN Tracker will request the VPN gateway's certificate. This setting should normally be turned on. Only turn off this setting if your VPN gateway has trouble dealing with certificate requests from connecting clients. In that case, you'll need to have the VPN gateway's certificate in your keychain.

Related Settings: Basic > Authentication > Certificate

Availability: The setting is only available for certificate-based authentication.

Verify Remote Certificate

This setting can be used to temporarily disable certificate verification for debugging purposes.



Do not turn off this option except for debugging purposes!

Related Settings: Basic > Authentication > Certificate

Availability: The setting is only available for certificate-based authentication.

NAT-Traversal

Set NAT-Traversal to "Automatic".

There are some very specific circumstances in which you may need to change the setting, please read and understand → *VPN and Network Address Translation (NAT)*, before making any changes to this setting.

Availability: always

Connection Timeout

The default settings are more than sufficient for most setups. Only in extreme network environments with high packet loss or extremely high latency (think

“connecting from a space probe back to earth”) will you have to increase the timeout (and/or the number of times VPN Tracker attempts to resend a packet).

Availability: always

Interoperability

Send INITIAL-CONTACT Message

For some devices it is necessary to send this message when establishing a VPN connection in order to tell the VPN gateway to clean up “old” VPN connections. However, other devices will disconnect all other VPN users upon receiving this message (in particular if multiple VPN users connect from the same public IP address, or when users share an XAUTH account).

Availability: According to the selected device profile.

Advertise as Dead Peer Detection Capable

VPN Tracker supports Dead Peer Detection (DPD) to detect if the other end of the connection is no longer responding. When this setting is turned on, VPN Tracker will tell the VPN gateway that it supports Dead Peer Detection.

For most VPN gateways (whether they support Dead Peer Detection or not) this option should be turned on. Only turn it off if you suspect that VPN Tracker offering to perform Dead Peer Detection causes a problem on the VPN gateway, or if the VPN gateway’s Dead Peer Detection implementation is broken.

Related Settings: Advanced > Interoperability > Perform active Dead Peer Detection

Availability: According to the selected device profile.

Perform active Dead Peer Detection every ... seconds, if necessary

If the VPN gateway is Dead Peer Detection capable, but does not perform Dead Peer Detection itself, VPN Tracker can perform Dead Peer Detection.

For most VPN gateways (whether they support Dead Peer Detection or not) this option should be turned on. Only turn it off if you suspect that VPN Tracker performing Dead Peer Detection causes problems (such as unexpected disconnects because the VPN gateway is not responding but the VPN is working anyway).

Related Settings: Advanced > Interoperability > Advertise as Dead Peer Detection Capable

Availability: According to the selected device profile.

Use ... as the Application Version during Mode Config

When performing Mode Config (or EasyVPN), VPN Tracker will identify itself as “VPN Tracker 7”. Identifying as a different client or version may be necessary to work with some VPN gateways.

To identify as a specific client, simply enter its name and version, e.g. “Cisco Systems VPN Client 4.8.0:Linux”.

Related Settings: Basic > Network Configuration

Availability: Available with a custom device profile or a Cisco device profile when using Mode Config or EasyVPN.

Send Cisco Unity Vendor ID

This setting is necessary in order to use certain Cisco-specific extensions, such as EasyVPN. Turn on this setting if you are connecting to a Cisco device using a custom device profile (it is not necessary to use this setting when using one of the Cisco device profiles shipping with VPN Tracker).

Availability: Only available using a custom device profile. The setting is automatically used in all Cisco device profiles.

Send Cisco Firewall Attribute during Mode Config

When checked, VPN Tracker will send a special attribute indicating the presence of a firewall. This may help to successfully connect to some Cisco devices.

Related Settings: Basic > Network Configuration

Availability: Only available with custom device profiles or Cisco device profiles when using EasyVPN (or Mode Config with the “Send Cisco Unity Vendor ID” option turned on).

Establish a Shared Tunnel to 0.0.0.0/0 for Split-Tunneling

When checked, VPN Tracker will establish a single tunnel (Security Association, SA) to 0.0.0.0/0 and set suitable routes to achieve split-tunneling. This can noticeably speed up connecting to a Cisco VPN gateway with multiple remote networks using EasyVPN and resolve issues with idle timeouts for those connections.

This setting should be turned on when connecting to Cisco devices using Cisco EasyVPN.

Related Settings: Basic > Network Configuration

Advanced > Phase 2 > Establish a separate phase 2 tunnel for each remote network

Availability: Available when EasyVPN is used and “Establish a separate phase 2 tunnel for each remote network” is turned off.

IPv6

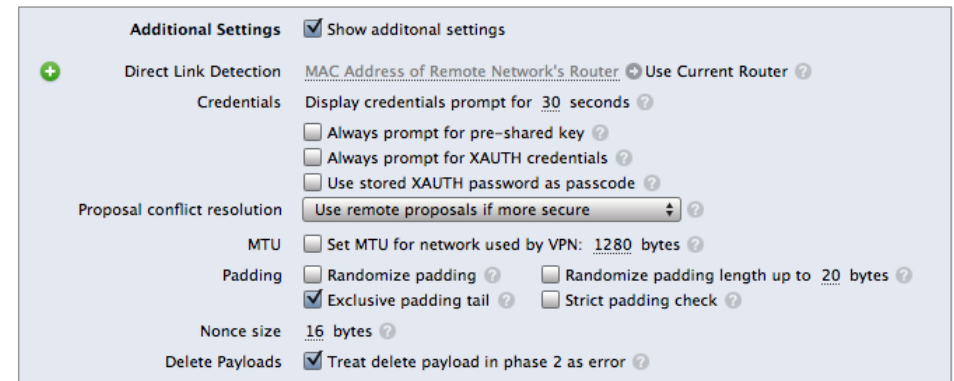
Prefer IPv6 VPN gateway address, if available

You will not normally need to change this setting. If your VPN gateway is reachable through IPv6 and its host name resolves to an IPv4 address as well as to an IPv6 address, VPN Tracker will use the IPv6 address if this setting is turned on.

Related Settings: Basic > VPN Gateway

Availability: According to the selected device profile.

Additional Settings



Direct Link Detection

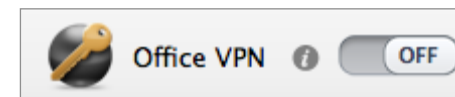
This setting helps VPN Tracker detect when your Mac is physically attached to the network you normally connect to through VPN so you can use Secure Desktop and the Network Scanner in those locations.

For example, if you use your MacBook at the office without VPN, and from home with VPN, you can teach VPN Tracker to recognize when you are connected to your office network and no VPN is needed.

To teach VPN Tracker to recognize a direct link to your remote network:

- ▶ Physically connect your Mac to the remote network of your VPN connection (e.g. if you connect to your office through VPN, connect your Mac to the office network). Direct link detection also works with wireless networks.
- ▶ Open VPN Tracker and go to Advanced > Additional Settings > Direct Link Detection
- ▶ Click “Use Current Router”

VPN Tracker will detect the local router’s unique hardware address (MAC address) and remember it. The next time you are connected to this network and try to connect to the VPN, VPN Tracker will know that no VPN is needed:



You'll also see a message in the log when Direct Link Detection is active:

```
13:44:16 Direct Link to Remote Network
Your computer is currently directly connected to the remote network. It is therefore not necessary (and not possible) to connect the VPN.
Please note: VPN Tracker detects if your computer is directly connected to the remote network through the Direct Link Detection setting.
Should you have accidentally entered your current network there, simply remove it again to resolve the problem.
```

If you have a very complex network, you can teach VPN Tracker about more than one router. Simply click the green plus button to add more input fields.

Related Settings: Basic > Network > Remote Network(s)

Availability: always

Display credentials prompt for ... seconds

When VPN Tracker asks for VPN connection passwords (pre-shared key, Extended Authentication (XAUTH) credentials), the password prompts are only displayed for a limited of time to indicate that most VPN gateways will drop the connection attempt if the password is not supplied within a short time.

If necessary, this setting lets you increase the time a password prompt is being displayed. This can be useful for accessibility purposes, or when dealing with devices that request the next passcode from a passcode generator token (which can take up to 1 minute).

Do not increase the timeout unless you have a specific reason to do so. Most devices will no longer expect a password after 15-60 seconds and thus the connection attempt will fail if entering a password takes too much time.

Availability: always

Always prompt for the pre-shared key Always prompt for XAUTH credentials

If enabled VPN Tracker will always prompt for the pre-shared key and/or XAUTH password, even if one is stored in keychain.

If a pre-shared key or password is stored, the password entry field will be pre-filled with this password, but the "Store in Keychain" checkbox will be turned off in order to prevent you from accidentally replacing the stored password.

This settings is useful if

- ▶ You are using a VPN gateway that asks you to fill the password field with password/pin + a generated one-time passcode. In that case, you can store the password/pin in keychain and have it pre-filled, and then add the generated code every time you connect.
- ▶ You sometimes need to connect as a different XAUTH user but still want your "regular" XAUTH user account to be stored in keychain.

Availability: always

Use stored XAUTH password as passcode

A VPN gateway can ask for an XAUTH password or for a generated one-time passcode. Since it does not make sense to store **one-time** passcodes in keychain, VPN Tracker does not offer this option by default.

However, some VPN gateways incorrectly ask for a passcode even though they actually expect a password. In that case, enable this option to permit storing the password in keychain etc.

Availability: always

Proposal Conflict Resolution

When VPN Tracker and the VPN gateway disagree about the lifetime or the Perfect Forward Secrecy (PFS) setting, VPN Tracker can choose to accept the VPN gateway's proposal instead of insisting on its own settings (in which case the connection attempt would fail).

Use remote proposals

VPN Tracker will use whatever settings the VPN gateway suggests, even if they are less secure

Use remote proposals if more secure (strict)

VPN Tracker will use the settings the VPN gateway suggests if they are at least as secure as the current settings in VPN Tracker

Use remote proposals if more secure

VPN Tracker will use the settings the VPN gateway suggests if they are at least as secure as the current settings in VPN Tracker. If the lifetime mismatches and the VPN gateway's lifetime is longer, VPN Tracker will attempt to use its own

(shorter) lifetime. While this will allow initial connectivity, it may lead to the connection being dropped unexpectedly later on.

Never use remote proposals

VPN Tracker will treat a mismatch as an error and stop connecting.

Related Settings: Advanced > Phase 2 > Lifetime
Advanced > Phase 2 > Perfect Forward Secrecy (PFS)

Availability: Only available using a custom device profile.

Manually set MTU for network used by VPN

VPN Tracker normally uses an MTU (maximum transfer unit) of 1280 bytes. In extremely rare circumstances it may be necessary to decrease the MTU further in order to avoid fragmentation of network packets.

If you have to decrease the MTU, please be aware that the MTU in VPN Tracker needs to be set to 52 bytes less than the actual MTU that can be used.

Availability: always

Padding

These settings determine how VPN Tracker handles cryptographic padding. **You should not change these settings unless instructed to do so by technical support.**

Availability: Only available using a custom device profile.

Nonce Size

Determines the size of the nonce for the Diffie-Hellman (DH) key exchange. **You should not change this setting unless instructed to do so by technical support.**

Availability: Only available using a custom device profile.

Treat delete payloads in phase 2 as errors

A delete payload normally is a strong indication that the VPN gateway has terminated the connection, and the only recovery possible is a reconnect of the VPN. This setting disables this recovery mechanism and will cause dead connections for almost all users. **Do not uncheck this setting unless instructed to do so by technical support.**

Availability: Only available using a custom device profile.

Actions Tab

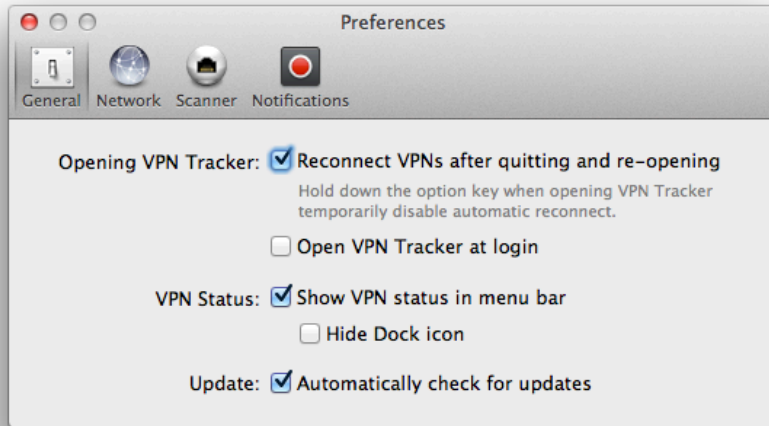
The actions tab is explained in detail in → *Working with VPN Tracker*

Export Tab

A description of the export settings can be found → *Exporting Connections*.

VPN Tracker Preferences

General Preferences



Reconnect VPNs after quitting and re-opening

VPN Tracker can remember and reconnect the VPNs that were connected when you quit the application or restarted your Mac.

If you would like to temporarily disable automatic reconnect, hold down the option key while opening VPN Tracker.

Open VPN Tracker at login

VPN Tracker can open automatically at login. By default, VPN Tracker will open hidden. If you would like VPN Tracker to be visible on login, uncheck the "Hide" checkbox in System Preferences > Users & Groups > Login Items.

To connect certain VPNs at launch, check the box on the Actions tab of the VPN(s) you would like to connect.

Show VPN status in menu bar

VPN Tracker can show its status in the menu bar. For more information about what the menu bar item can do, see → *Menu Bar Item*

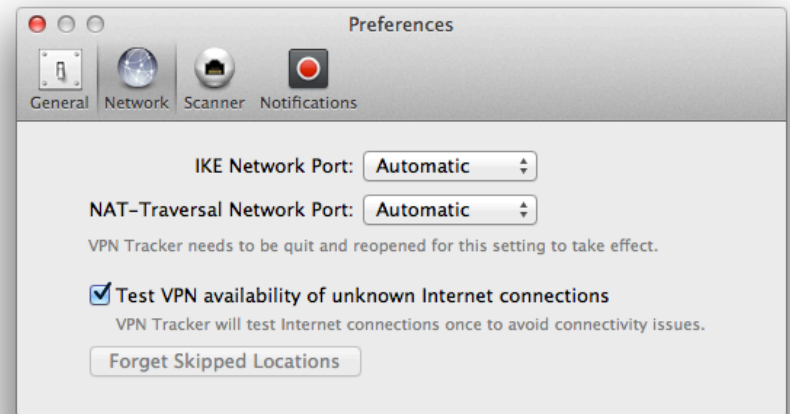
Hide Dock Icon

Check this box if you want to control VPN Tracker entirely from the menu bar, with no application icon being displayed in the Dock.

Automatically check for updates.

VPN Tracker can automatically check for updates so you never miss out on important improvements to VPN Tracker. When an update is available, you will be asked if you would like to download and install the update.

Network Preferences



Network Ports

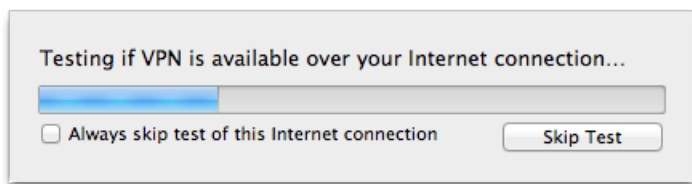
VPN Tracker normally connects **from** network port 500, the default port for IPsec VPN, and port 4500 for NAT-Traversal (VPN Tracker always connects **to** ports 500, and 4500 on the VPN gateway end).

If VPN Tracker cannot connect **from** ports 500 and 4500 because they are already in use, it will resort to alternate ports if the setting is "Automatic."

In case you need VPN Tracker to always use a specific port (and treat it as an error, should that port not be available), you may set specific network ports here.

Test VPN availability of unknown Internet connections

VPN Tracker automatically tests if VPN is available over your current Internet connection before attempting to connect to your VPN. **Testing occurs only once for any given Internet connection** – for example, the first time you connect from a hotel's Internet access, VPN Tracker will test the connection. When returning to that hotel a few months later, VPN Tracker usually won't need to test again.



Testing your Internet connection enables VPN Tracker to adjust its NAT-Traversal settings depending on what the Internet connection supports. For more information about NAT-Traversal and how VPN Tracker is testing your Internet connection, see → *VPN and Network Address Translation (NAT)*

It is strongly recommended to let VPN Tracker test unknown Internet connections for their VPN availability: If VPN Tracker knows what NAT-Traversal mechanisms are supported by your current Internet connection, VPN Tracker will be able to avoid many common connectivity issues automatically.

However, if you are using VPN Tracker to secure access to internal networks from another internal network (e.g. securing a corporate Wi-Fi network), it may be necessary to disable testing (entirely or just when connected to this particular network).

To disable testing for all Internet connections (not recommended):

- ▶ Open Preferences > Network
- ▶ Uncheck "Test VPN availability of unknown Internet connections"

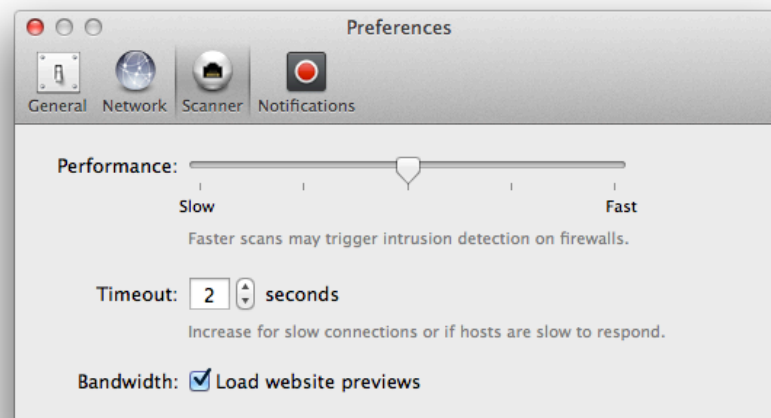
To disable testing for the current Internet connection:

- ▶ Open the VPN Availability Test (Tools > VPN Availability Test)
- ▶ Click "More Details"
- ▶ Check "Ignore test result"

You can also choose to skip the test while the test is in progress.

To reset all skipped Internet connections and start testing again, click the button "Forget Skipped Locations" in Preferences > Network.

Scanner Preferences



Performance

This setting determines how aggressively VPN Tracker scans a network. On the slowest setting, VPN Tracker will only scan a single service on a single host at a time. On the fastest setting, many services and hosts will be scanned concurrently. This could trigger intrusion detection systems on the VPN gateway or other firewalls, and cause you to be blocked from network access.

A medium setting is recommended for good performance and low risk of being blocked.

Timeout

By default, VPN Tracker waits for two seconds to receive a response from a service. Increase the timeout for slow (high latency) network connections or if hosts on the remote network are slow to respond.

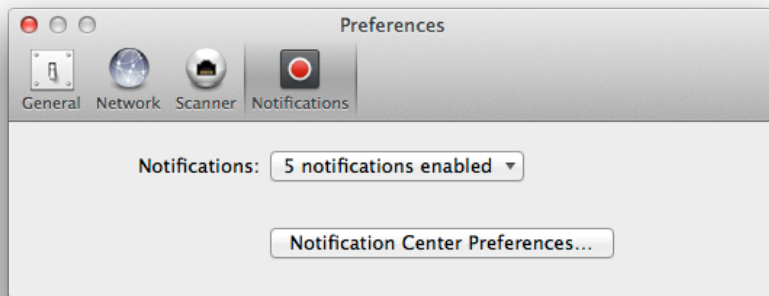
Increasing the timeout significantly increases the time a scan will take to complete, but may also increase the accuracy of the results.

Load website previews

VPN Tracker shows previews of websites that the Network Scanner has found. Loading these previews may require a significant amount of network bandwidth if there are many and/or complex websites.

You may want to disable website previews if you are being charged for network bandwidth, or if you are on a very low-bandwidth Internet connection.

Notification Preferences



VPN Tracker can display notifications for events such as VPN connect and disconnect, status changes, or errors.

Use the “Notifications” popup to select those events that you would like to be notified about.

If you are using OS X 10.8 or newer, you can customize the way notifications are displayed in Notification Center Preferences.



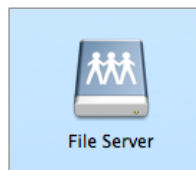
If you have [Growl](#) installed, VPN Tracker will use Growl to enable even more customization of notifications. In that case, you will find all notification-related settings in Growl Preferences.

Secure Desktop Reference

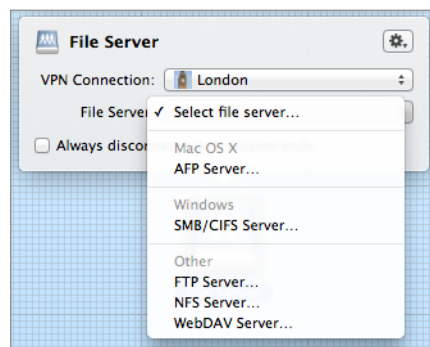
This chapter describes the items available in Secure Desktop and how to customize them to get the most out of Secure Desktop.

Connecting to File Servers

To connect to a file server (network share), drag the “File Server” item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that is required for accessing this file server (here, the VPN is called “London”).
- ▶ Select the type of server that you would like to connect to, and enter its IP address. There are several types of file servers that VPN Tracker can connect to.



If your VPN has a working → *Remote DNS* setup, you can use a host name instead of an IP address.

If there are file servers currently connected to your Mac, they will be shown in the list and you can select one of those directly.

When you’re done setting up the file server, leave the Secure Desktop’s edit mode and click the item to test it.

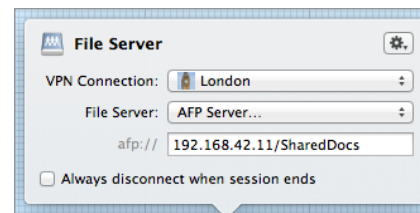
You will be prompted for your username and password (if required), as well as for the volume(s) on the file server that you would like to access¹.



It is not possible to use Bonjour or NETBIOS names for accessing file servers. Please use IP addresses instead, or set up → *Remote DNS* to be able to use DNS host names.

OS X File Servers (AFP)

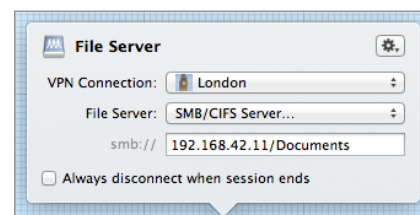
Select “AFP Server” if your file server is a Mac running OS X, or an Apple Time Capsule. Some NAS (Network Attached Storage) devices can be accessed using AFP, please refer to your device’s documentation for details.



In addition to the server’s address, you may optionally enter the volume after the address, separated by a forward slash (“/”), e.g. 192.168.42.11/SharedDocs.

Windows File Servers (SMB/CIFS)

Select “SMB/CIFS Server” if your file server is running Windows, or if you are connecting to a file server with Windows-compatible network shares. Many NAS devices offer SMB services.



In addition to the server’s address, you may optionally enter the share after the address, separated by a forward slash (“/”), e.g. 192.168.42.11/Documents.

FTP Server

Select “FTP Server” if you are connecting to a file server running the File Transfer Protocol (FTP). Many NAS devices offer FTP services, and FTP is a popular protocol for uploading files to web hosting.

NFS Server

Select “NFS Server” if you are connecting to a file server running the Network File System (NFS). You must specify the entire path to the network share, e.g. 192.168.42.11/export/docs.

WebDAV Server

Select “WebDAV Server” if you are connecting to a file server running the WebDAV protocol. WebDAV is a popular protocol for uploading files to web hosting.

¹ For NFS file servers, the share must be specified in the Secure Desktop file server item.

Opening Websites and other URLs

You can use the Web Browser item in Secure Desktop to open a website.



The Web Browser item can open **any URL**, e.g. telnet://, ssh://, etc., so if you have an application that can open URLs, you can use it here.



When you're done setting up the item, leave Secure Desktop's edit mode and click the item to test it.



URLs will open in the default application registered on the Mac for the URL. The icon will automatically change to reflect the application that will open. You can set a custom icon by clicking the gear icon in the upper right corner of the inspector.

Accessing Windows PCs using Microsoft Remote Desktop

You can put Microsoft Remote Desktop connections onto your Secure Desktop to share the screen of remote Windows PCs.

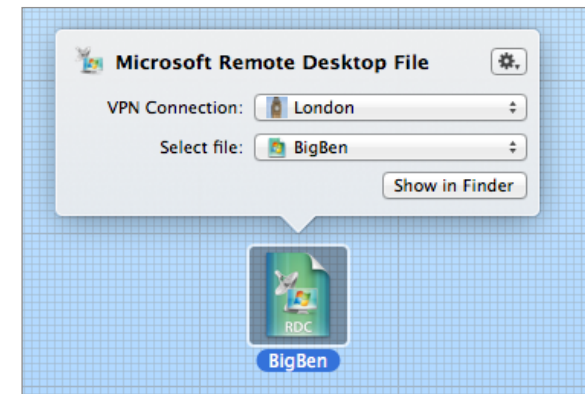


Microsoft Remote Desktop for Mac needs to be installed and a connection set up in order to use this feature. Microsoft Remote Desktop can be downloaded at <http://www.microsoft.com/mac>

To share the screen of a Windows PC, drag the "Microsoft Remote Desktop" item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that is required for accessing the Windows PC (here, the VPN is called "London").
- ▶ Select the Microsoft Remote Desktop connection needed to connect to the Windows PC (here, the connection is called "BigBen").



When you're done setting up the Microsoft Remote Desktop item, leave Secure Desktop's edit mode and click the item to test it.



If you haven't set up a Microsoft Remote Desktop connection yet, you can do so right within the Microsoft Remote Desktop for Mac application. Any connections configured there can be selected in Secure Desktop.

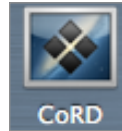
Accessing Windows PCs using CoRD

CoRD is an alternative to Microsoft Remote Desktop for Mac to share the screen of remote Windows PCs right from Secure Desktop.

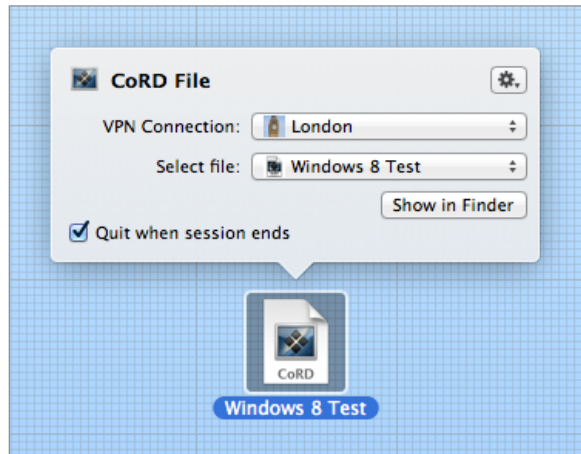


CoRD needs to be installed and a connection set up in order to use this feature. CoRD can be downloaded at <http://cord.sf.net>.

To share the screen of a Windows PC, drag the “CoRD” item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that is required for accessing the Windows PC (here, the VPN is called “London”).
- ▶ Select the Microsoft Remote Desktop connection needed to connect to the Windows PC (here, the connection is called “Windows 8 Test”).



When you’re done setting up the CoRD item, leave Secure Desktop’s edit mode and click the item to test it.

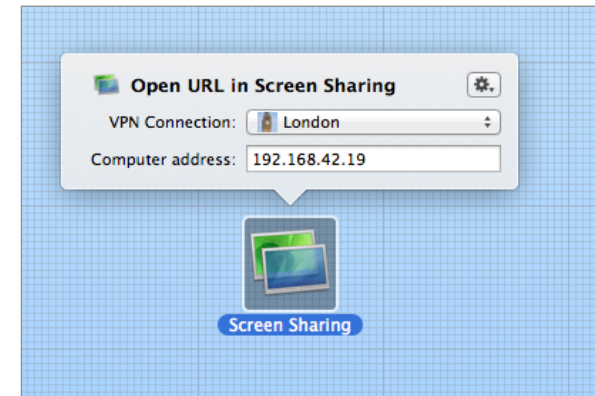
Accessing your Macs using Screen Sharing (VNC)

All modern versions of OS X support Screen Sharing through VNC. Make sure Screen Sharing is enabled on the Mac whose screen you would like to share (System Preferences > Sharing). VN

To share the screen of a Mac, drag the “Screen Sharing” item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that is required for accessing the Mac (here, the VPN is called “London”).
- ▶ Enter the IP address of the Mac whose screen you would like to share. If your VPN has a working → *Remote DNS* setup, you can use a host name instead of an IP address.



When you’re done setting up the Screen Sharing item, leave Secure Desktop’s edit mode and click the item to test it.

Accessing your Macs using Apple Remote Desktop (ARD)

If you have Apple Remote Desktop (ARD) installed, you can use it to manage remote Macs over VPN right from Secure Desktop.



Apple Remote Desktop needs to be installed and the Mac needs to be in one of its computer lists in order to use this feature. More information about Apple Remote Desktop can be found at <http://www.apple.com/remotedesktop>

To observe or control a remote Mac, drag the “Apple Remote Desktop” item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that is required for accessing the Mac (here, the VPN is called “London”).
- ▶ Choose if you would like to control or observe the Mac.
- ▶ Enter the IP address of the Mac that you would like to manage. If your VPN has a working → *Remote DNS* setup, you can use a host name instead of an IP address.



When you’re done setting up the Apple Remote Desktop item, leave Secure Desktop’s edit mode and click the item to test it.



The Apple Remote Desktop item will fall back to VNC Screen Sharing if the computer you’re attempting to connect to is not in one of Apple Remote Desktop’s computer lists.

Accessing FileMaker Databases

If you have FileMaker installed, you can open remote (and local) databases and run scripts from Secure Desktop.

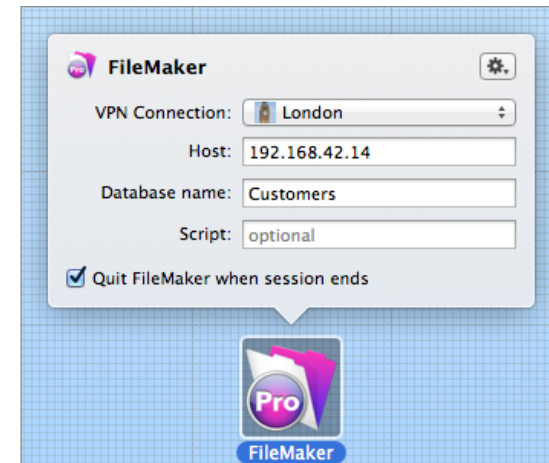


FileMaker needs to be installed to use this feature. Information about FileMaker can be found at <http://www.filemaker.com>

To open a FileMaker database, drag the “FileMaker” item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that is required for accessing the FileMaker server (here, the VPN is called “London”).
- ▶ Enter the IP address of the FileMaker server. If your VPN has a working → *Remote DNS* setup, you can use a host name instead of an IP address.
- ▶ Enter the name of the database.
- ▶ If you would like to run a script when opening the database, enter its name.

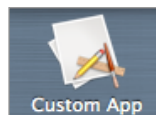


When you’re done setting up the FileMaker item, leave Secure Desktop’s edit mode and click the item to test it.

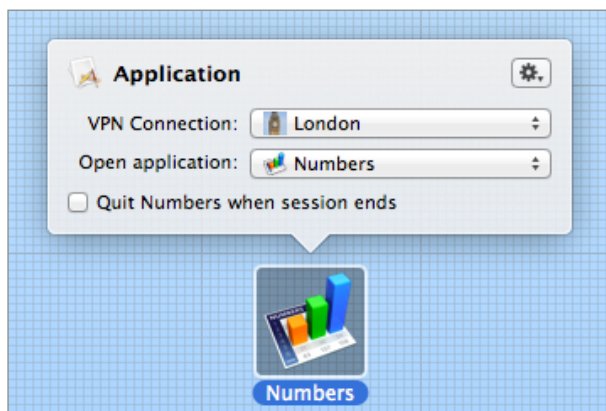
Opening Mac and Windows Applications

You can open any Mac application from Secure Desktop, as well as Windows applications from Virtual Machines running Windows.

To open any application, drag the “Custom App” icon to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that you would like to connect prior to opening the app (here, the VPN is called “London”).
- ▶ Select the app to open (here: Numbers).
- ▶ Optionally, check the box to quit the app before the VPN is disconnected.



When you’re done setting up the application item, leave Secure Desktop’s edit mode and click the item to test it.



The VPN settings determine which network traffic goes through the VPN. Putting an application on your Secure Desktop will **not** cause its traffic to go through the VPN **unless** the associated VPN is configured to send that traffic through the VPN. More information can be found in → *Topology*.

Windows Applications

To add Windows applications from your virtual machines, locate the folder that mirrors your VM’s applications (e.g. Documents > Virtual Machines > Your Windows Machine > Applications) and choose the application from there.

You need a virtual machine software that makes Windows applications accessible through the OS X file system and the VM needs to be set up to share your Mac’s network connection.

Administrating OS X Server

You can manage OS X Server from Secure Desktop using the OS X Server app.

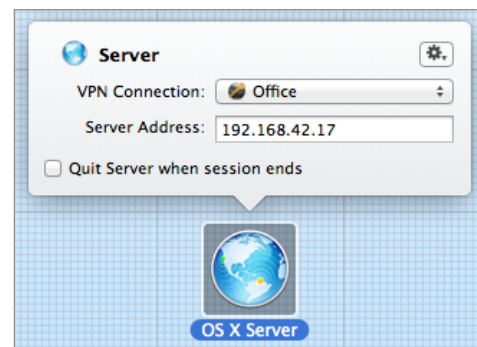


The OS X Server application needs to be installed on your Mac (OS X server itself does not have to be installed), and the server needs to be listed in the app to be accessible to Secure Desktop.

To add OS X Server, drag the “OS X Server” icon to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that is required for accessing the server (here, the VPN is called “Office”).
- ▶ Enter the IP address of the server. If your VPN has a working → *Remote DNS* setup, you can use a host name instead of an IP address.



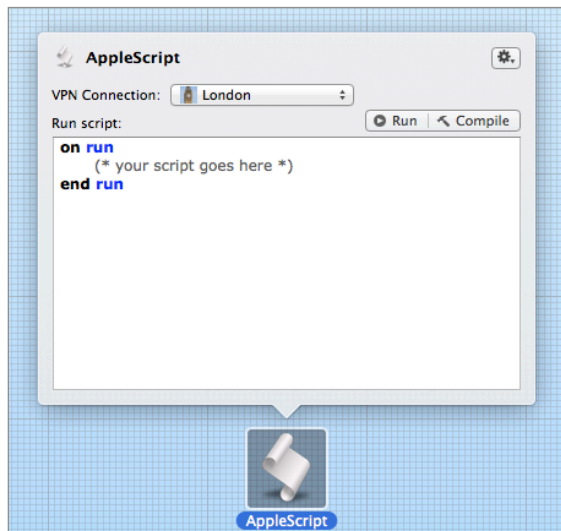
Automating Tasks Using AppleScript

You can use AppleScript to automate repetitive tasks that need a VPN: Uploading files to a server, getting the newest data from a database, sending files to a service for processing, etc.

To add an AppleScript, drag the “AppleScript” item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



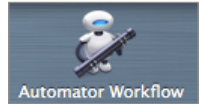
- ▶ Select the VPN that you would like to connect prior to running the script (here, the VPN is called “London”).
- ▶ Enter the AppleScript. Use the Run and Compile buttons to test your script.



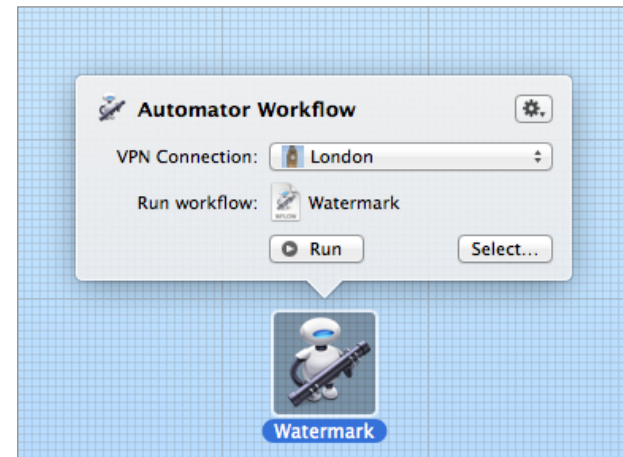
Automating Tasks Using Automator

You can add Automator workflows to Secure Desktop to automate repetitive tasks that require a VPN. Uploading files to a server, getting the newest data from a database, sending files to a service for processing, etc.

To add an Automator workflow, drag the “Automator” item to your Secure Desktop. Secure Desktop must be in → *Edit Mode* to add items.



- ▶ Select the VPN that you would like to connect prior to running the Automator workflow (here, the VPN is called “London”).
- ▶ Drag the workflow into the inspector, or use the Select button to select a workflow from disk. Use the Run button to test your workflow.



If your script or workflow needs a file server to be connected, you can either connect the file server as part of the script, or use an → *Action* in your VPN to connect the file server.

Accessing Files & Printers over VPN

Using Finder to Connect to File Servers

Secure Desktop or Finder? Your Choice!

Secure Desktop lets you connect to file servers right from within VPN Tracker (→ [Learn More](#)). However, if you wish, you can of course also use the Finder to connect to your file servers.

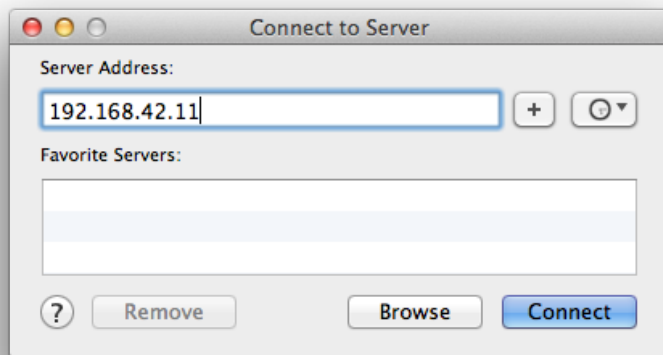
To connect to your file server (network share):

- ▶ Switch to Finder by clicking its icon in the Dock
- ▶ Choose Go > Connect to Server from the menu bar on top of your screen. You can also use the keyboard shortcut ⌘-K



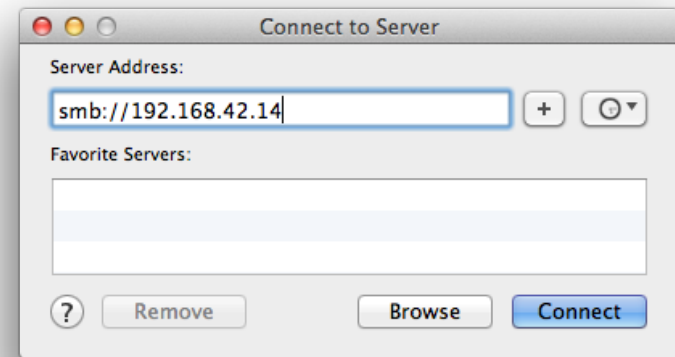
If your file server is a Mac (AFP):

- ▶ Enter the IP address (e.g. 192.168.42.4)¹ of your server in the “Server Address” field and click “Connect”.



If your file server is running Windows (SMB/CIFS):

- ▶ Enter “smb://” followed by the IP address (e.g. 192.168.42.14)¹ of your server and click “Connect”.



You will be prompted for your username and password (if required), as well as for the volume(s) on the file server that you would like to access.

If your VPN has a working → *Remote DNS* setup, you can use a host name instead of an IP address.

I don't know my file server's IP address. Can't I just access my file servers via the Finder Sidebar?

When using a VPN connection, your servers won't show up in the Finder sidebar because the network protocols used for this service, Bonjour and NETBIOS, do not travel over the VPN.

If you don't know your file server's IP address, you can easily find it out next time you're in your office network:

Open Tools > Ping Host and enter your file server's name. After a few seconds, VPN Tracker should tell you the file server's IP address. Again, this will only work when you're actually in your office network, not if you're connected via VPN.

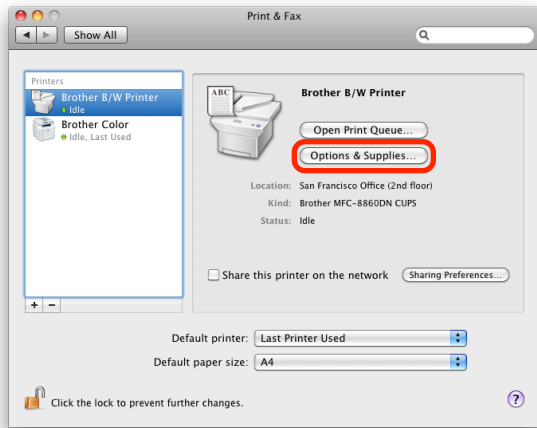
¹ If your VPN connection uses remote DNS, you can also use a DNS host name instead of an IP address.

Printing over VPN

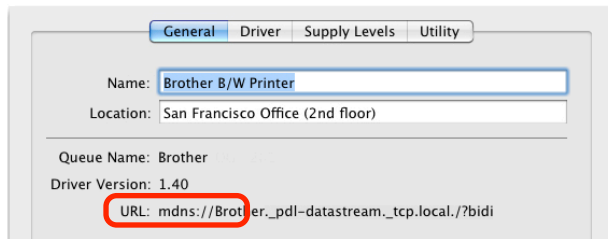
It is possible to print to network printers over VPN. The trick is to use the printer's IP address (or DNS host name) when setting up the printer on your Mac. It is not possible to use printers that have been auto-detected by Bonjour over the VPN because your Mac does not know their IP address or DNS host name.

If you have a network printer that's already set up on your Mac, check if it is using Bonjour:

- ▶ Open System Preferences "Print & Fax".
- ▶ Click "Options & Supplies".



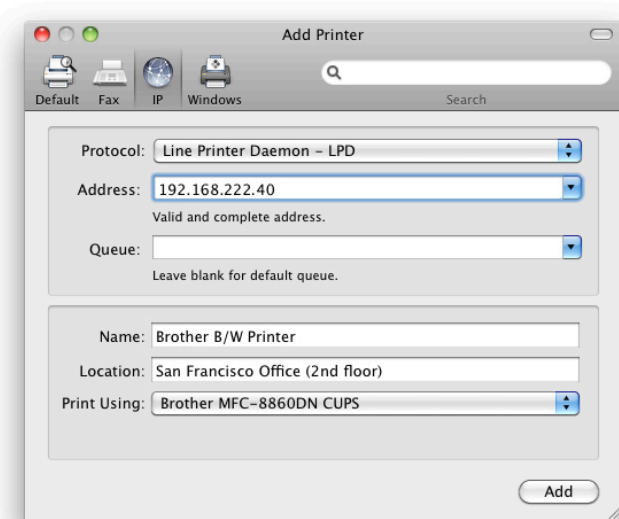
- ▶ If the URL starts with "mdns://" your printer is a Bonjour printer and you will need to add it again using its IP address.



Adding a Network Printer for Printing Over VPN

Before starting, make sure you know your printer's IP address or DNS host name. To help your Mac auto-detect the printer settings, it is helpful if your Mac is physically connected to your remote network or connected to the VPN while you set up the printer.

- ▶ Open System Preferences "Print & Fax".
- ▶ Click the plus button to add a new printer.



- ▶ Select whether your printer is an IPP, LPD or HP JetDirect printer (your printer's administrator or its manual will be able to tell you which it is).
- ▶ Enter your printer's IP address.
- ▶ Wait until OS X has determined your printer type. This works only if the printer is reachable. If not, you'll have to select the printer driver yourself.
- ▶ Click "Add" to add the new printer.



In VPN Tracker Pro, you can add printers directly from the Network Scanner's results.

L2TP / PPTP Connections **PRO**

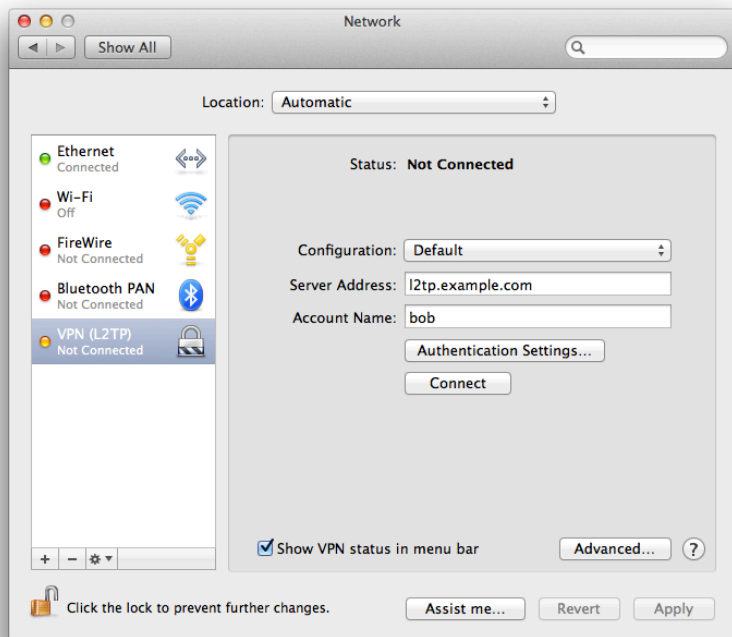
Find out how to integrate OS X L2TP / PPTP connections into VPN Tracker.

OS X has a built-in VPN client that can connect to L2TP and PPTP VPNs. In VPN Tracker Pro, these connections are automatically integrated into the sidebar so you can use all your VPN connections from one place.

Setting up a new L2TP or PPTP VPN in OS X

- ▶ Open System Preferences > Network.
- ▶ Click the '+' icon.
- ▶ Select the VPN interface and your type of VPN.
- ▶ Configure the VPN and click "Apply".

For further information, please click the question mark to open OS X Help.



The VPN will automatically appear in the sidebar in VPN Tracker under "Other VPN Connections" and can be controlled from there.



OS X L2TP/PPTP VPN connections are always associated with a specific network location. VPN Tracker therefore only shows those VPN connections that belong to the current network location (System Preferences > Network > Location).

VPN and Network Address Translation (NAT)

VPN Tracker provides reliable VPN connectivity, even through routers that perform Network Address Translation (NAT). This chapter explains the technical background of Network Address Translation, the different NAT-Traversal methods available, and how VPN Tracker makes everything work seamlessly.

Private IP Addresses

In the early years of the Internet, each computer had a worldwide unique IP address. When it became clear that the Internet was growing rapidly and would soon run out of IP addresses, certain blocks of IP addresses were reserved for use on private networks. These private IP addresses can be used over and over again in different private networks, they do not have to be unique worldwide.

The following IP address ranges are reserved for private use:

First IP Address	Last IP Address	Number of IP Addresses
192.168.0.0	192.168.255.255	65 536
10.0.0.0	10.255.255.255	16 777 216
172.16.0.0	172.31.255.255	1 048 576

Network Address Translation (NAT)

When a computer with a private IP address accesses the Internet, it sends the request through its local router. The local router cannot simply forward the request to the Internet: The sender's private IP address is not unique outside its particular private network – in fact there can be millions of computers on the Internet worldwide that have the same private IP address at any given

moment! Instead, it makes a few changes to the sender's information in the request:

- ▶ It replaces the private IP address of the sender with its own public IP address.
- ▶ If necessary, it changes the outgoing network port number so no other computer communicating with the recipient of the request uses the same network port (it also remembers which port was used by which computer on its private network).

It then forwards the request to the Internet.

When responses come back, the process needs to be reversed. Responses will come back on the same network port the request was sent out. The router can therefore easily look up which computer sent the original request.

- ▶ The router replaces the recipient of the response with the private IP address of the computer who sent the original request.
- ▶ If it had to change the network port, the router puts back the original network port.

It then forwards the response to its private network.

The entire process is called Network Address Translation (NAT). If you have a DSL or wireless router (e.g. an AirPort Base Station) at home, it is very likely performing Network Address Translation. In most offices, hotels, and Internet cafes you will be connecting to a private network that has a NAT router for accessing the Internet.

NAT-Traversal

Network Address Translation used to be a problem for VPN connections: Once the VPN is established, the actual communication over the VPN uses a network protocol called ESP. Unlike the TCP and UDP network protocols you may be familiar with, ESP does not use network ports. Since NAT depends on being able to use network ports to identify the recipient of an incoming response, it cannot work with ESP out of the box. Two methods have been developed to deal with NAT-Traversal:

IPSec Passthrough

For IPSec Passthrough, the local router needs to know about IPSec VPN and the ESP protocol. In its most basic form, the router simply sends all ESP traffic to the last host on its network that talked to the VPN gateway. Most NAT routers have some limitation on their IPSec Passthrough capability, for example it often cannot support more than a single computer connecting to the VPN.

Since the local router takes care of everything, no special support is required on the VPN gateway or the VPN client.

NAT-Traversal

With NAT-Traversal, VPN Tracker wraps ESP into regular UDP packets (which have port numbers and can easily be handled by NAT routers). On the other end, the VPN gateway needs to remove the UDP “wrapper” before it can decrypt the VPN communication.

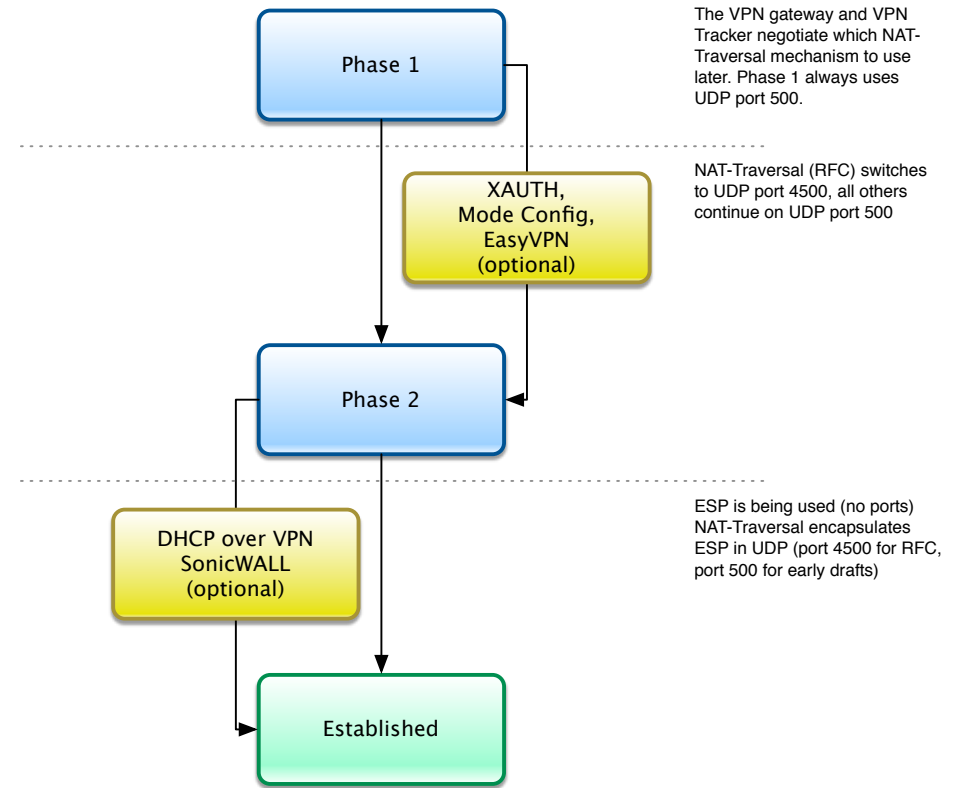
There are several versions of NAT Traversal. Some VPN gateways support only one form of NAT-Traversal, and some, particularly older or low-end VPN gateways, support none. **VPN Tracker and the VPN gateway automatically negotiate which form of NAT-Traversal, if any, to use.**

Since VPN Tracker and the VPN gateway take care of everything, no special support for NAT-Traversal is required from the local router, though firewall rules or firmware issues could prevent NAT-Traversal from working.



If you are buying a new VPN gateway, make sure it supports all forms of NAT-Traversal – it is very likely that you will encounter Internet connections that require NAT-Traversal to work.

The following diagram shows how a VPN is established using different NAT-Traversal mechanisms:



NAT-Traversal: Earlier Draft Versions vs. RFC

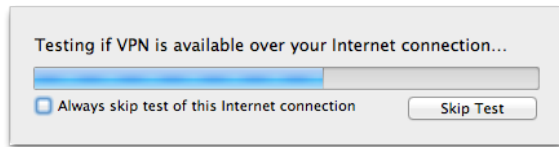
The early NAT-Traversal draft versions sent UDP packets on network port 500, the same port also used for the initial connection process of the VPN. This sometimes caused trouble with NAT routers that simply discarded UDP packets on network port 500.

To deal with this problem, the final NAT-Traversal standard (RFC) changed the network port for performing NAT-Traversal to the (non-privileged) UDP network port 4500.

Testing for NAT-Traversal Support

As you can see from the diagram, there are a several points where the local router could interfere with the VPN. **VPN Tracker can detect such problems and in most cases work around them by selecting the most suitable NAT-Traversal method for any given situation – whether it's a hotel, an Internet cafe or your home Wi-Fi network.**

VPN Tracker runs a test the first time it encounters a new local router (that's the progress bar you see before the VPN connection is established).



Even though it may take a short moment, it's very important to run the test! It only needs to run a single time at any given location.

What does the test do?

The test connects to a VPN gateway at equinix using all possible NAT-Traversal methods: IPsec Passthrough, NAT-Traversal (early drafts), and NAT-Traversal (RFC). VPN Tracker tests and remembers which methods worked, and from then on it will only use the working methods.

Should VPN Tracker ever encounter a situation where the local router blocks all VPN traffic, or where the properties of the local Internet connection would require a form of NAT-Traversal that is not supported by your VPN gateway, it will specifically tell you so.

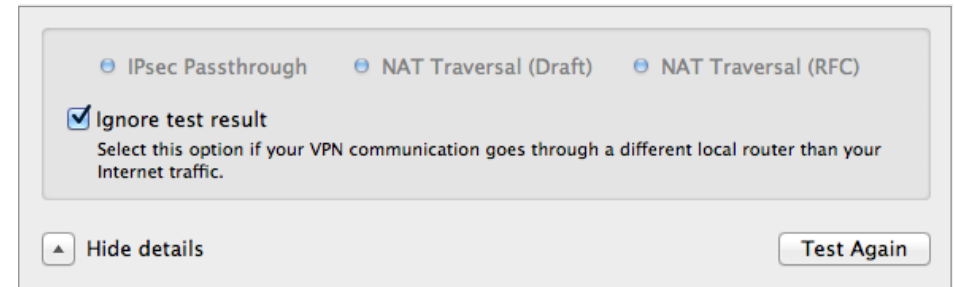
In what situations is the automatic test not sufficient?

The automatic test will work in almost all situations. It will help you to get hassle-free VPN connectivity at Internet cafes, hotels, airports – basically in all those places where you have little time and encounter routers that may not support all NAT-Traversal methods.

There is one specific situations in which the availability test may not give accurate results: If communication to your VPN gateway goes through a different router than Internet traffic, or is treated differently (firewall rules etc.).

Since the test VPN gateway is located on the Internet, the test results reflect the connectivity from your location to VPN gateways on the Internet, but may not be accurate for your VPN gateway if it is handled differently.

In that case, you can open the VPN Availability Test (Tools > Test VPN Availability) and tell VPN Tracker to ignore the test results for this specific location.



To disable testing entirely, go to → *VPN Tracker Preferences*.

What if my local router changes? What if a firmware upgrade changes its capabilities?

If you exchange the router for a different device, VPN Tracker will notice automatically (it uses the router's hardware address (MAC) to remember which routers it already tested).

If only the firmware is updated, or you are using an Internet connection where NAT-Traversal happens off-site at your Internet Service Provider (ISP), VPN Tracker cannot detect a change automatically. In that case, please open the VPN Availability Test (Tools > Test VPN Availability) and repeat the test.

Certificates and Smart Cards

This chapter describes how VPN Tracker can be integrated into a PKI (Public Key Infrastructure) using digital certificates or smart cards.

Getting Started

To use certificates with VPN Tracker, you will need certificates and a VPN gateway that can authenticate users through X.509 certificates (RSA signatures).

Obtaining Certificates

If you have an existing Public Key Infrastructure (PKI) that uses certificates:

- ▶ Certificates (and private keys for the client/user certificates) need to be available in a format supported by the OS X keychain. If your users already have their certificates in their OS X keychain, there's nothing that needs to be done.

If you have an existing Public Key Infrastructure (PKI) that uses smart cards:

- ▶ Software is required to make your smart card certificates available in OS X through the keychain. If you have already installed your vendor's driver or software, you can easily determine if it satisfies this requirement by checking if your smart card appears as a keychain in the OS X Keychain Access application (Applications > Utilities > Keychain Access)
- ▶ If your vendor does not provide the necessary software, there may be a third party solution available

If you do not have an existing Public Key Infrastructure (PKI) in place:

- ▶ Use the Certificate Assistant built into the OS X Keychain Access application to create certificates (Keychain Access > Certificate Assistant). Some VPN gateways also can create and export certificates.

VPN Gateway Prerequisites

- ▶ Your VPN gateway must support the use of authentication based on digital certificates (X.509 certificates)

- ▶ Configure your VPN gateway for certificate-based authentication. Refer to your vendor's documentation for details.

What about Tokens?

We are using the term "smart card" to describe both an actual smart card that is placed into a card reader, and a USB token with a non-removable smart card chip that plugs directly into your Mac. From VPN Tracker's perspective, there is no difference if the smart card chip is accessed through a card reader, or built into a USB token.

There is also another type of token on the market: These tokens generate a one-time code (e.g. RSA SecurID). When using such tokens, the VPN gateway usually request the code through Extended Authentication (XAUTH). To use such tokens in VPN Tracker, simply set up your VPN gateway according to your vendor's instructions and enable XAUTH in VPN Tracker.

Certificate Management in OS X

To use certificates with VPN Tracker, the certificates must be available in a keychain. This chapter therefore will first cover the basics of certificate management using the keychain on OS X, before showing how to include certificates in VPN Tracker.



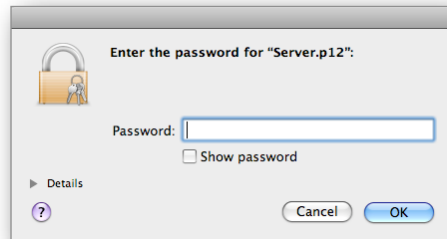
In OS X, certificates (and their private keys) are stored in keychains. Keychains are managed using the Keychain Access application (found in Applications > Utilities).

A keychain protects the private key by only permitting access if the keychain has been unlocked using the appropriate password. Also, if applications attempt to access a private key in a keychain for the first time, the user is asked to permit access, even if the keychain is unlocked. By default, a user has a single keychain, the login keychain, protected with their password. It is possible to change the login keychain's password to a different one, and to create additional keychains.

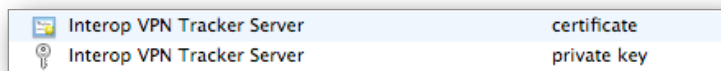
Importing Certificates

Certificates can be imported into a OS X keychain using any of the usual certificate formats (PEM, DER, PKCS#7, PKCS#12). To import a certificate, simply double-click the certificate file, or choose File > Import Items... in Keychain Access.

If the certificate contains a private key and the certificate file is protected by a password, you will be asked for this password:



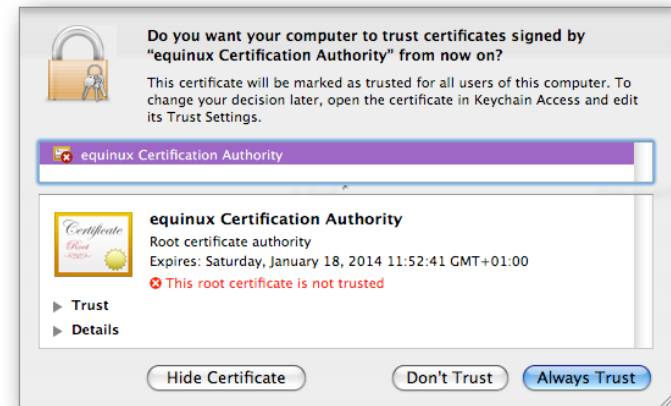
If the certificate contained a private key, you will see both the certificate and its private key in the list after importing. A combination of a certificate and its private key is called an identity in OS X.



If only the public part of the certificate was imported, you will see only the certificate listed after importing.

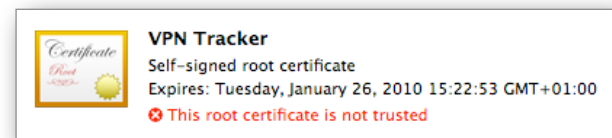
Importing Certificate Authorities

Importing a certificate authority works the same as importing a regular certificate. After importing, you will be asked if you want to trust this certificate authority. If you choose "Always Trust", certificates signed by this certificate authority will be trusted automatically in the future.



Checking a Certificate's Trust

Keychain Access easily lets you see if a given certificate is trusted, and if not, why not. Simply select the certificate and examine the top part of the Keychain Access window (if the details are not visible, choose View > Show Summary to display them):



Which Certificates Do I Need?

To use certificate-based authentication in VPN Tracker, you will need the following certificates in your OS X keychain:

VPN Client:

- ▶ VPN client (VPN user) certificate **and**
- ▶ Private key belonging to the VPN client (VPN user) certificate

VPN Gateway (optional):

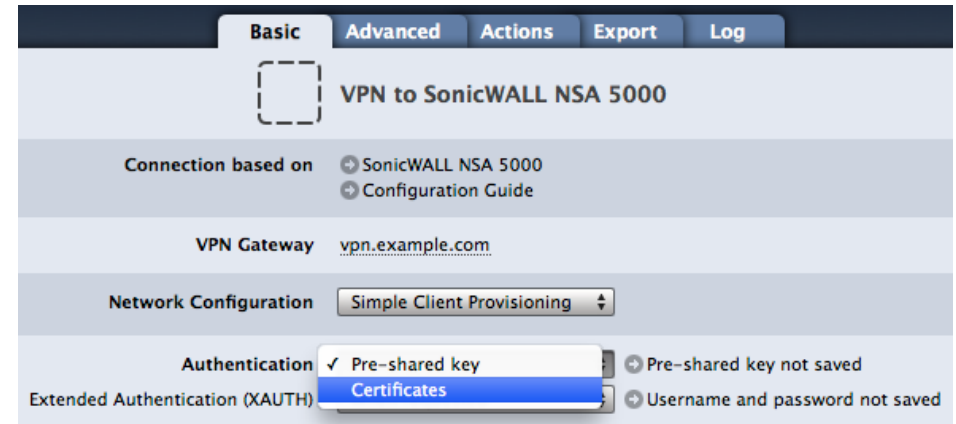
- ▶ VPN gateway's certificate (without the private key) **or**
- ▶ Certificate authority (CA) that signed the VPN gateway's certificate. Its certificate must be set as trusted on your Mac. The VPN gateway must be capable of sending its actual certificate upon connection initiation, which is the case for almost all VPN gateways



You can easily check if a private key is available for a given certificate by selecting the "My Certificates" category in the left column in Keychain Access. If a certificate appears there, it has a private key available.

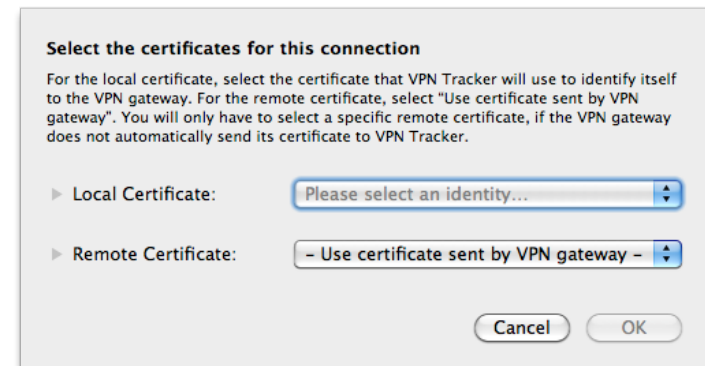
Selecting Certificates in VPN Tracker

If you have not yet done so, set the authentication method to "Certificates".



Make sure your VPN gateway is already configured for certificate-based (X.509 certificates / RSA signatures) authentication before starting to configure VPN Tracker.

In the certificate selection window, select your certificate(s). The certificate selection window opens automatically if you are not yet using certificates. If you have already selected some certificates earlier, click the "Edit" button on the Basic tab.



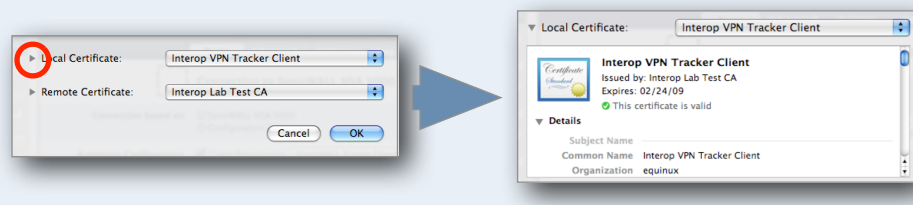
Local Certificate

The local certificate is the certificate you are using to identify to the VPN gateway as a user/client. It is sometimes called client certificate or user certificate. A private key is required for the local certificate, since it must sign messages to the VPN gateway.

If you cannot find your certificate here even though you have imported it into the OS X keychain, make sure the corresponding private key is also available in the keychain. You can easily check that by selecting the “My Certificates” category in Keychain Access. If it does not appear there, the private key is missing.

Inspecting a Certificate

Click the triangle to see the details for the selected certificate.



Remote Certificate

The remote certificate is the VPN gateway’s certificate. A private key is not needed. There are two options:

- ▶ Select your VPN gateway’s certificate **or**
- ▶ Select “Use certificate supplied by peer”¹ to use the certificate the VPN gateway sends upon connecting, and verify it against the certificate authorities installed on your Mac. If verification fails, you will be prompted to verify the certificate manually.



Even though CA certificates may show up in the list, you should selecting a CA certificate as the remote certificate will not work.

Certificates and Exported Connections

Certificates are never included in an exported connection, since most organizations with a PKI infrastructure already have well-established (and secure) procedures of distributing certificates to users in place. The exported connection **does include** the information **which certificates** were selected.

When exporting an unlocked connection:

- ▶ If the selected certificates are present on the recipient’s Mac, VPN Tracker will use these certificates
- ▶ If the selected certificated do not exist on the recipient’s Mac, the recipient will be able to select different certificates

When exporting a locked connection:

- ▶ The recipient will not be able to edit their VPN connection settings. It is therefore important to select the correct certificates before exporting

Identifiers Based on Certificates

It is possible to use the information from certificates as an identifier for the VPN connection. To do this, set the Local (Remote) Identifier to Local (Remote) Certificate”. VPN Tracker will then use the certificate’s information (such as subject, organization, country etc.) as the identifier for the connection.

Certificate Identifier Types

A “Local (Remote) Certificate” identifier will technically be sent as an identifier of type ASN.1 Distinguished Name (DN). On your VPN gateway, such an identifier may also be called simply Distinguished Name or Subject.

Advanced Certificate Settings

There are several settings on the Advanced tab that influence how certificates are verified. These options should usually be left enabled. For more information, see the → *Settings Reference*

¹ Locked connections require the VPN gateway certificate or a trusted CA that signed the certificate. If your VPN gateway is not capable of transmitting its certificate, the certificate is always required.

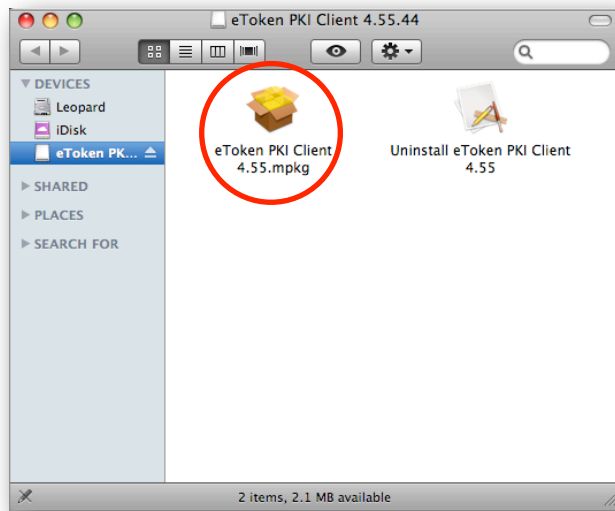
Using Smart Cards

Storing certificates on a smart card provides even more security than using certificate-based authentication with certificates stored locally on your Mac. This chapter shows how to set up smart card based authentication with VPN Tracker using Aladdin eToken.

Vendor Software Installation

To access your smart card on your Mac, you will first have to install the software provided by your smart card vendor. The following steps show the software installation for Aladdin eToken.

Step 1 – Start the installation

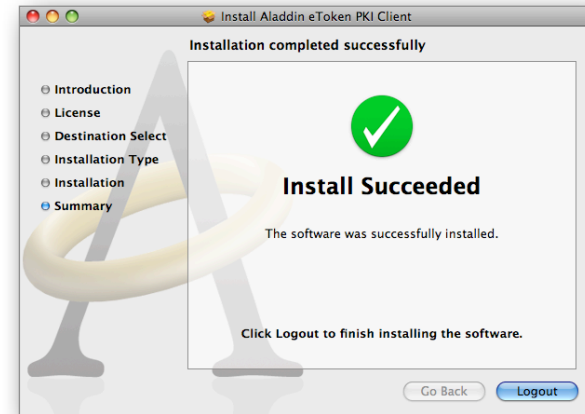


- ▶ The installation program will guide you through the necessary installation steps
- ▶ Make sure to carefully read all instructions

Step 2 – Follow the installation wizard



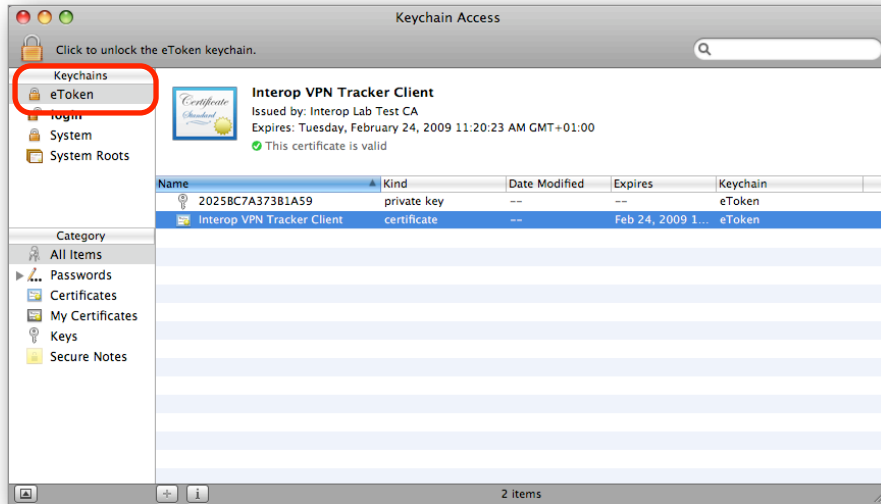
Step 3 – Finish the installation by logging out



- ▶ When the installation has finished, you will have to log out (and log back in) to complete the installation.
- ▶ The installation will provide you with two software applications. The **PKI-Monitor** allows you to monitor the attached eToken devices, and the **eToken Properties** application lets you configure your eToken and import certificates onto the device.
- ▶ Please refer to your vendor's documentation for additional details on how to set up your smart card or token.

Verifying Access

To verify that you are indeed able to access your smart card or token through the OS X keychain, start the Keychain Access application. You should be able to find your token in the keychain list on the left (use “View > Show Keychain List” if the keychain list is not displayed).



If you have not done so yet, import or create your certificates on the smart card now. The best way to do this is through the software tools provided by your smart card vendor (such as through the eToken Properties application when using Aladdin eToken). Make sure that the private key for your client/user certificate is also present on the smart card. You can easily verify this by selecting the “My Certificates” category in Keychain Access. If the certificate is displayed there, the private key is available.

Selecting Smart Card Certificates in VPN Tracker

Selecting a certificate located on a smart card works exactly the same as selecting a regular certificate. Please refer to → *Selecting Certificates in VPN Tracker* for details.

Troubleshooting Certificates

Most errors can be resolved quickly by carefully following the hints given by VPN Tracker in its log. However, here are some frequently asked questions that cannot be covered by the log hints.

My connection works fine, but I am prompted for my keychain password or keychain access permission every time I connect

- ▶ If you are using a smart card, this behavior is inherent to the way smart cards work, storing the access code is not possible
- ▶ If you are using normal certificates stored in your keychain, please make sure the OS X keychain subsystem has write access to the keychain that your certificate and private key are stored in, and to the folder the keychain is in. You can run the **Keychain First Aid** tool that is part of Keychain Access (Keychain Access > Keychain First Aid) to verify permissions.

My certificate is only in the Remote Certificate list, however, I want to select it as the Local Certificate

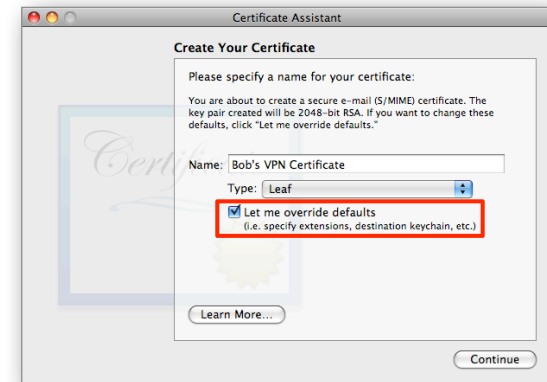
A certificate that is to be used as the local certificate must have its private key stored in the keychain (or on the smart card). If a certificate does not have a private key available, it will not be displayed in the Local Certificates list.

I cannot add my certificate to the keychain: Keychain Access keeps complaining that the certificate already exists, but I searched for it and it is not there!

A certificate is uniquely identified by the combination of issuer (i.e. the certificate authority signing it), and the serial number. If your keychain already contains a certificate issued by the same certificate authority with the same serial number, it will not be possible to add another certificate with the same issuer and serial number combination, even though the rest of the certificate may be completely different.

Unfortunately, it is fairly easy to accidentally create certificates with duplicate serial numbers when using the OS X Certificate Assistant. There are two possible ways of resolving this problem:

- ▶ Recreate the certificate using an unused serial number (in Certificate Assistant, check the box "Let me override defaults" to modify the serial number)



- ▶ If you do not have the possibility to recreate the certificate, put the offending certificate into a separate keychain

I followed the advice in the log and double-checked my configuration, but the connection still fails

Before contacting technical support, please run the Keychain First Aid tool that is part of Keychain Access (Keychain Access > Keychain First Aid). Then try connecting again. Also double-check that you have selected the correct certificates. A certificate authority (CA) certificate should never be selected as the local or remote certificate.

If the problem persists, and you need to contact us, please include the following information with your support request:

- ▶ A **Technical Support Report** from VPN Tracker (Help > Technical Support Report...)
- ▶ Screenshots of the VPN configuration on your VPN gateway, if possible
- ▶ The **output of the Terminal command** `security dump-keychain` (preferred), or **screenshots of the details of all certificates** used with the connection: In Keychain Access, select each certificate and choose "File > Get Info". Make sure the details are visible (click the triangle, if necessary) and take a screenshot of the details.

Choosing the Right VPN Device

What You're Looking For

Whether you're shopping for a new device or are trying to find out if your existing router can act as a VPN gateway, these are the magic words you'll want to look for – if they're mentioned in the manual or data sheet, the device is probably suitable:

- ▶ IPsec VPN Access
- ▶ IPsec Tunnels
- ▶ <any number of> IPsec Tunnels
- ▶ <any number of> IPsec VPN connections
- ▶ <any number of> IPsec VPN users
- ▶ <any number of> IPsec SAs

Misleading Feature Names

If a device lists *only* one or more of the following features, it probably cannot act as a VPN gateway:

- ▶ IPsec Passthrough
- ▶ VPN Passthrough
- ▶ IPsec NAT-Traversal

These features indicate that the device is capable of letting IPsec VPN connections pass through. They do not indicate whether the device is capable of offering VPN services itself.

Other Types of VPNs

- ▶ L2TP or L2TP/IPsec
- ▶ PPTP

If your device offers only these types of VPNs, it may be possible to use the limited VPN client built-in to OS X. VPN Tracker lets you control these connections from inside VPN Tracker. Other VPN types, such as OpenVPN and proprietary SSL VPNs are not supported.

Apple Airport Base Stations

AirPort base stations are only capable of passing through VPN connections, but do not provide VPN services (i.e. act as a VPN gateway) themselves. If you are using an AirPort base station, you will need to buy a dedicated VPN gateway to replace or work alongside your Airport base station.

Recommended Devices

Now for the big question: Which device do we recommend?

Unfortunately there is no generic answer to this question. There are a lot of factors you'll need to consider, such as the number of VPN users you need to support, the type of Internet connection you have, etc.

Generally speaking, the most important features are

- ▶ Robust support for client-to-gateway connections (some older or low-end VPN gateways are designed to provide only a single gateway-to-gateway VPN that requires static IP addresses on both ends of the connection).
- ▶ Support for all forms of NAT-Traversal.
- ▶ Reasonable level of security (at least 3DES encryption, better AES, SHA-1 hash algorithms, better SHA-2, DH groups 2 and 5, better higher).
- ▶ If you expect more than one VPN user: Support for Extended Authentication (XAUTH) and a form of client provisioning (Mode Config, Cisco EasyVPN, SonicWALL DHCP over VPN, WatchGuard MobileUser VPN).

The technical support team at equinix has extensive experience with a large number of VPN gateways, so please feel free to email us with a brief outline of your requirements, and a list of devices you're considering, and we'll be happy to give you our take on them!

<http://vpntracker.com/support>

Further Resources

VPN Tracker

VPN Tracker Interoperability Website

Up-to-date information about device compatibility and detailed configuration guides for many popular VPN gateway devices.

<http://vpntracker.com/interop>

VPN Tracker Support Website

Large database of Frequently Asked Questions (FAQs), as well as downloads and the possibility to contact technical support.

<http://vpntracker.com/support>

VPN Tracker Deployment Guide

Deployment resources and best practices.

<http://www.vpntracker.com/goto/vpntmanualdeployment>

Computer Networking and VPNs

The TCP/IP Guide

An book on networking and the most popular networking protocols. Also available for free to read online.

<http://www.tcpipguide.com>

Wikipedia

- ▶ Internet Protocol (IP)
http://en.wikipedia.org/wiki/Internet_Protocol
- ▶ Subnets and Network Addressing:
<http://en.wikipedia.org/wiki/Subnetwork>
- ▶ Private IP Addresses
http://en.wikipedia.org/wiki/Private_network
- ▶ Network Address Translation (NAT)
http://en.wikipedia.org/wiki/Network_address_translation

- ▶ DNS
http://en.wikipedia.org/wiki/Domain_Name_System
- ▶ IPsec
<http://en.wikipedia.org/wiki/IPsec>

Keyboard Shortcuts

Here are some of the most useful keyboard shortcuts supported by VPN Tracker.

Action	Shortcut
Managing connections	
Start connection	⌘-Return
Reconnect	⌘-Option-Return
Edit Secure Desktop	⌘-Shift-E
New Connection	⌘-N
New Secure Desktop	⌘-Shift-N
New Group	⌘-Option-N PRO
Delete Connection or Secure Desktop	⌘-⌫
Tools	
Test VPN Availability	⌘-Option-W
Ping Host	⌘-Option-P
Lookup Host	⌘-Option-L
Export & Deployment	
Import Connection	⌘-Shift-i
Export Connection	⌘-E PRO
Show Export Settings	⌘-Option-E PRO

Action	Shortcut
Window shortcuts	
Open Log	⌘-L
Show / Hide Main Window	⌘-0
Show / Hide Connection Details	⌘-i
Switch Tabs Status/Accounting/Scanner/Log	⌘-1 to ⌘-4
Switch Edit Tabs Basic/Advanced/Actions/Notes	⌘-Option-1 to 4
Application shortcuts	
Preferences	⌘-,
Hide VPN Tracker	⌘-H
Hide Others	⌘-Option-H
Close Window	⌘-W
Minimize Window	⌘-M
Quit VPN Tracker	⌘-Q